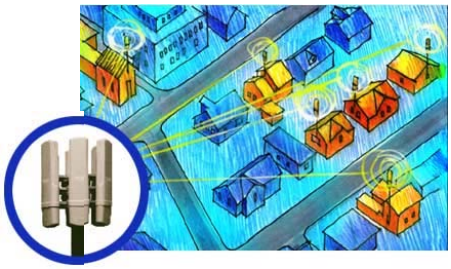
MOTOROLA
intelligence everywhere™



Canopy™ System User Guide

Sys-UG-en
Issue 1
March 2005

CANOPY™
Motorola Wireless Broadband Platform

Notices

See the following information:

- important regulatory and legal notices in Section 36 on Page 400.
- personal safety guidelines in Section 15 on Page 127.

Trademarks, Product Names, and Service Names

MOTOROLA, the stylized M Logo and all other trademarks indicated as such herein are trademarks of Motorola, Inc.® Reg. U.S. Pat & Tm. Office. Canopy is a trademark of Motorola, Inc. All other product or service names are the property of their respective owners.

© 2005 Motorola, Inc. All rights reserved.

http://www.motorola.com/canopy

TABLE OF CONTENTS

GUIDE TO THIS USER GUIDE

1 New in This Issue 25

1.1 Products Covered by This User Guide 25

1.2 Products Not Covered by This User Guide 25

1.3 Software Compatibility Described in This User Guide 25

2 Using This User Guide 26

2.1 Finding the Information You Need 26

2.1.1 Becoming Familiar with This User Guide 26

2.1.2 Searching This User Guide 29

2.1.3 Finding Parameter and Field Definitions for Module Web Pages 29

2.2 Interpreting Typeface and Other Conventions 31

2.3 Getting Additional Help 32

2.4 Sending Feedback 32

UNDERSTANDING CANOPY NETWORKS

3 Advancing from Research to Implementation 34

4 Realizing a Wireless Backhaul Network 35

5 Exploring the Scope of Solutions 37

5.1 Components 37

5.1.1 Access Point Module 37

5.1.2 Access Point Cluster 37

5.1.3 Subscriber Module 38

5.1.4 900-MHz AP and SM 38

5.1.5 Backhaul Module 39

5.1.6 45-Mbps Backhaul Module 39

5.1.7 Power Indoor Unit for 45-Mbps Backhaul Module 40

5.1.8 T1/E1 Multiplexer 41

5.1.9 Cluster Management Module 2 (Part 1008CK) 42

5.1.10 Cluster Management Module micro (Part 1070CK) 42

5.1.11 Accessory Components 43

5.2 Frequency Band Ranges 47

5.3 Canopy Product Comparisons 48
5.3.1 Canopy Product Applications 48
5.3.2 Link Performance and Encryption Comparisons 49
5.3.3 Cluster Management Product Comparison 50
5.4 Antennas for Connection to 900-MHz Modules 50
5.4.1 Certified Connectorized Flat Panel Antenna from Motorola 51
5.4.2 Other Certified Connectorized Flat Panel Antenna 51
5.4.3 Third-party Certified Connectorized Flat Panel Antenna 51
5.5 Bandwidth and Authentication Manager Software 52
5.6 License Manager Software 52
5.7 Specifications and Limitations 52
5.7.1 Radios 52
5.7.2 Cluster Management Products 53
5.7.3 300SS Surge Suppressor 54

6 Differentiating Among Components 55
6.1 Interpreting Part Number 56
6.2 Interpreting Serial Number 57

7 Canopy Link Characteristics 59
7.1 Understanding Bandwidth Management 59
7.1.1 Downlink Frame Contents 59
7.1.2 Uplink Frame Contents 59
7.1.3 Frame Structure 59
7.1.4 Media Access Control and AP Capacity 60
7.1.5 Canopy Slot Usage 61
7.1.6 Data Transfer Capacity 61
7.1.7 QoS Parameters 61
7.1.8 Maximum Information Rate (MIR) 62
7.1.9 Committed Information Rate 63
7.1.10 Bandwidth from the SM Perspective 63
7.1.11 Interaction of Burst Allocation and Sustained Data Rate Settings 64
7.1.12 High-priority Bandwidth 64
7.1.13 Allocations to Downlink and Uplink 65
7.1.14 Software and Hardware Scheduling 65
7.1.15 Settable AP Broadcast Repeat Count 67
7.2 Understanding Synchronization 68

7.2.1 GPS Synchronization 68
7.2.2 Passing Sync in a Single Hop 70
7.2.3 Passing Sync in an Additional Hop 70

8 Meeting Link Requirements 73
8.1 AP-SM Links 73
8.1.1 AP-SM Link Distances 73
8.1.2 AP-SM Data Transfer 73
8.2 BH-BH Links 76
8.2.1 BH-BH Link Distances 76
8.2.2 BH-BH Data Transfer 77

9 Previewing Network Configurations 79
9.1 Viewing Typical Layouts 79
9.2 Viewing Case Studies 81

10 Accessing Features 82
10.1 Activating Features 86
10.1.1 Fixed License Keys 86
10.2 Enabling Features 87

11 Acquiring Proficiencies 88
11.1 Understanding RF Fundamentals 88
11.2 Understanding IP Fundamentals 88
11.3 Acquiring a Canopy Demonstration Kit 88
11.3.1 900-MHz Demonstration Kit 88
11.3.2 2.4-GHz Demonstration Kit 89
11.3.3 5.2-GHz Demonstration Kit 89
11.3.4 5.4-GHz Demonstration Kit 90
11.3.5 5.7-GHz Demonstration Kit 90
11.4 Acquiring a Canopy Starter Kit 91
11.4.1 900-MHz Starter Kit 91
11.4.2 2.4-GHz Starter Kit 91
11.4.3 5.2-GHz Starter Kit 92
11.4.4 5.4-GHz Starter Kit 92
11.4.5 5.7-GHz Starter Kit 93
11.5 Evaluating Canopy Training Options 93
11.6 Attending On-line Knowledge Sessions 94

12 Engineering Your RF Communications 96

12.1 Anticipating RF Signal Loss 96

12.1.1 Understanding Attenuation 96

12.1.2 Calculating Free Space Path Loss 96

12.1.3 Calculating Rx Signal Level 96

12.1.4 Calculating Fade Margin 97

12.2 Analyzing the RF Environment 98

12.2.1 Mapping RF Neighbor Frequencies 98

12.2.2 Anticipating Reflection of Radio Waves 99

12.2.3 Noting Possible Obstructions in the Fresnel Zone 99

12.2.4 Radar Signature Detection and Shutdown 100

12.3 Considering Frequency Band Alternatives 100

12.3.1 900-MHz Channels 101

12.3.2 900-MHz Single AP Available Channels 101

12.3.3 2.4-GHz Channels 101

12.3.4 5.2-GHz Channels 102

12.3.5 5.4-GHz Channels 102

12.3.6 5.7-GHz Channels 103

12.3.7 5.8-GHz Channels Available for 45-Mbps Backhaul Module 104

12.3.8 Example Channel Plans for AP Clusters 104

12.3.9 Multiple Access Points Clusters 106

12.4 Selecting Sites for Network Elements 107

12.4.1 Resources for Maps and Topographic Images 107

12.4.2 Surveying Sites 108

12.4.3 Assuring the Essentials 108

12.4.4 Finding the Expected Coverage Area 109

12.4.5 Clearing the Radio Horizon 109

12.4.6 Calculating the Aim Angles 109

12.5 Collocating Canopy Modules 110

12.6 Diagramming Network Layouts 111

12.6.1 Accounting for Link Ranges and Service Coverage 111

12.6.2 Accounting for Data Handling Requirements 113

12.6.3 Avoiding Self Interference 114

12.6.4 Avoiding Other Interference 115

13 Engineering Your IP Communications 116

13.1 Understanding Addresses 116
13.1.1 IP Address 116
13.2 Dynamic or Static Addressing 116
13.2.1 When a DHCP Server is Not Found 116
13.3 Network Address Translation (NAT) 117
13.3.1 NAT, DHCP Server, DHCP Client, and DMZ in SM 117
13.3.2 NAT Pass-through of VPN as L2TP over IPSec 122
13.4 Developing an IP Addressing Scheme 123
13.4.1 Address Resolution Protocol 123
13.4.2 Allocating Subnets 123
13.4.3 Selecting Non-routable IP Addresses 124

14 Engineering VLANs 125

BUILDING YOUR CANOPY NETWORK

15 Avoiding Hazards 127
15.1 Preventing Overexposure to RF Energy 127
15.1.1 Details of Calculations for Separation Distances and Power Compliance Margins 127
15.2 Redirecting Lightning Strikes 129
15.3 Conforming to Regulations 129
15.4 Protecting Cables and Connections 129

16 Testing the Components 131
16.1 Unpacking Components 131
16.2 Configuring for Test 131
16.2.1 Configuring the Computing Device for Test 131
16.2.2 Default Module Configuration 132
16.2.3 Component Layout 132
16.2.4 Diagnostic LEDs 133
16.2.5 CMM2 Component Layout 134
16.2.6 CMMmicro Component Layout 134
16.2.7 Standards for Wiring 136
16.2.8 Best Practices for Cabling 136
16.2.9 Recommended Tools for Wiring Connectors 137
16.2.10 Wiring Connectors 137
16.3 Configuring a Point-to-Multipoint Link for Test 138
16.3.1 Quick Start Page of the AP 139

16.3.2 Time & Date Page of the AP 141
16.3.3 Sessions Page of the AP 144
16.3.4 LUID Select Page of the AP 147
16.3.5 Status Page of the SM 148
16.3.6 Status Page of the AP 151
16.4 Configuring a Point-to-Point Link for Test 153
16.4.1 Quick Start Page of the BHM 154
16.4.2 Time & Date Page of the BHM 156
16.4.3 Sessions Page of the BHM 159
16.4.4 LUID Select Page of the BHM 162
16.4.5 Status Page of the BHS 163
16.4.6 Status Page of the BHM 166
16.4.7 Configuring a CMMmicro for Test 168
16.4.8 Status Page of the CMMmicro 174
16.4.9 Configuration Page of the CMMmicro 177
16.4.10 Configuring Modules for Connection to CMMmicro 184
16.4.11 Event Log Page of the CMMmicro 184
16.4.12 GPS Status Page of the CMMmicro 184
16.4.13 Port MIB Page of the CMMmicro 185

17 Preparing Components for Deployment 187
17.1 Correlating Component-specific Information 187
17.2 Ensuring Continuing Access to the Modules 187

18 Configuring for the Destination 189
18.1 Configuring an AP for the Destination 189
18.1.1 Configuration Page of the AP 189
18.1.2 IP Configuration Page of the AP 204
18.2 Configuring an SM for the Destination 206
18.2.1 Configuration Page of the SM 206
18.2.2 IP Configuration Page of the SM with NAT Disabled 215
18.2.3 IP Configuration Page of the SM with NAT Enabled 217
18.2.4 NAT Configuration Page of the SM with NAT Disabled 223
18.2.5 Advanced Network Configuration Page of the SM with NAT Disabled 224
18.2.6 NAT/Advanced Network Configuration Page of the SM with NAT Enabled 226
18.2.7 NAT Configuration Buttons with NAT Enabled 232
18.2.8 VLAN Configuration Page of the SM 232
18.3 Setting the Configuration Source 234

18.4 Configuring a BH Timing Master for the Destination 235
18.4.1 Configuration Page of the BHM 236
18.4.2 IP Configuration Page of the BHM 244
18.5 Configuring a BH Timing Slave for the Destination 246
18.5.1 Configuration Page of the BHS 246
18.5.2 IP Configuration Page of the BHS 254
18.6 Adjusting Transmitter Output Power 255

19 Installing Components 257
19.1 PDA Access to Canopy Modules 257
19.2 Installing an AP 259
19.3 Installing a Connectorized Flat Panel Antenna 260
19.4 Installing a GPS Antenna 260
19.4.1 Recommended Materials for Cabling the GPS Antenna 261
19.4.2 Cabling the GPS Antenna 262
19.5 Installing a CMM2 262
19.5.1 CMM2 Installation Temperature Range 262
19.5.2 Recommended Tools for Mounting a CMM2 262
19.5.3 Mounting a CMM2 262
19.5.4 Cabling a CMM2 263
19.5.5 Verifying CMM2 Connections 267
19.6 Installing a CMMmicro 268
19.6.1 CMMmicro Installation Temperature Range 268
19.6.2 Recommended Tools for Mounting a CMMmicro 268
19.6.3 Mounting a CMMmicro 268
19.6.4 Installing the Power Supply for the CMMmicro 269
19.6.5 Cabling a CMMmicro 270
19.6.6 Verifying CMMmicro Connections 271
19.7 Installing an SM 271
19.8 Verifying an AP-SM Link 275
19.9 Installing a Reflector Dish 275
19.9.1 Both Modules Mounted at Same Elevation 275
19.9.2 Modules Mounted at Different Elevations 276
19.9.3 Mounting Assembly 276
19.10 Installing a BH Timing Master 277
19.11 Installing a BH Timing Slave 279

19.12 Upgrading a BH Link to BH20 282
19.13 Verifying a BH Link 282

20 Verifying System Functionality 283

MANAGING YOUR CANOPY NETWORK

21 Growing Your Network 285
21.1 Monitoring the RF Environment 285
21.1.1 Spectrum Analyzer Web Pages 285
21.1.2 Graphical Spectrum Analyzer Display 286
21.1.3 Tabular Spectrum Analyzer Display 287
21.1.4 Updating the Spectrum Analyzer Page Readings 288
21.1.5 Using the AP as a Spectrum Analyzer 288
21.2 Considering Software Release Compatibility 289
21.2.1 Designations for Hardware and Firmware 289
21.2.2 Application, Boot, and FPGA Software Upgrades 290
21.2.3 System Release 6.1 Compatibility 291
21.2.4 BAM Software Compatibility 292
21.2.5 CMMmicro Software and Hardware Compatibility 293
21.2.6 MIB File Set Compatibility 293
21.3 Redeploying Modules 293
21.3.1 Wiring to Extend Network Sync 294

22 Securing Your Network 295
22.1 Isolating APs from the Internet 295
22.2 Encrypting Canopy Radio Transmissions 296
22.3 Managing Password Access 297
22.3.1 Configuring Display Only and Full Access Passwords 297
22.3.2 Setting and Changing Passwords 298
22.3.3 Overriding Forgotten IP Addresses or Passwords on AP, SM, or BH 300
22.3.4 Overriding Forgotten IP Addresses or Passwords on CMMmicro 302
22.4 Requiring SM Authentication 302
22.5 Filtering Protocols and Ports 303
22.5.1 Port Filtering with NAT Enabled 303
22.5.2 Protocol and Port Filtering with NAT Disabled 303
22.6 Encrypting Downlink Broadcasts 305

23 Managing Bandwidth and Authentication 306

23.1 Managing Bandwidth without BAM 306
23.2 Bandwidth and Authentication Manager (BAM) Services and Features 306
23.2.1 Bandwidth Manager Capability 306
23.2.2 Authentication Manager Capability 307

24 Managing through a Network Management Station (NMS) 308
24.1 Roles of Hardware and Software Elements 308
24.1.1 Role of the Agent 308
24.1.2 Role of the Managed Device 308
24.1.3 Role of the NMS 308
24.1.4 Dual Roles for the NMS 308
24.1.5 Simple Network Management Protocol (SNMP) Commands 308
24.1.6 Traps from the Agent 309
24.2 Management Information Base (MIB) 309
24.2.1 Cascading Path to the MIB 309
24.2.2 Object Instances 310
24.2.3 Management Information Base Systems and Interface (MIB-II) 310
24.2.4 Canopy Enterprise MIB 311
24.3 Configuring Modules for SNMP Access 312
24.4 Objects Defined in the Canopy Enterprise MIB 312
24.4.1 AP, SM, and BH Objects 312
24.4.2 AP and BH Timing Master Objects 314
24.4.3 SM and BH Timing Slave Objects 318
24.4.4 CMMmicro Objects 321
24.5 Objects Defined in the Canopy 45-Mbps BH Module MIB 324
24.6 Interface Designations in SNMP 325
24.7 Traps Provided in the Canopy Enterprise MIB 325
24.8 Traps Provided in the Canopy 45-Mbps BH Module MIB 326
24.9 MIB Viewers 326

25 Managing through the Canopy Network Updater Tool (CNUT) 327
25.1 CNUT Functions 327
25.2 Network Element Groups 327
25.3 Network Layers 327
25.4 Script Engine 328
25.5 Software Dependencies for CNUT 328
25.6 CNUT Download 329

26 Interpreting System Logs 330
26.1 Interpreting Messages in the Event Log Page 330
26.1.1 Time and Date Stamp 330
26.1.2 Event Log Data Collection 330
26.1.3 Messages that Flag Abnormal Events 332
26.1.4 Messages that Flag Normal Events 332
26.2 Interpreting Data in the AP Eval Data Page (SM, BHS) 333
26.2.1 AP Eval Data Parameters 334
26.3 Interpreting Data in the Sessions Page (AP, BHM) 335
26.3.1 Sessions Parameters 335
26.4 Interpreting Data in the GPS Status Page (AP, BHM) 337
26.5 Interpreting Data in the Ethernet Stats Page (All) 338
26.5.1 Ethernet Stats Parameters 338
26.6 Interpreting Data from Expanded Stats 340
26.6.1 Alignment Page (SM, BHS) 343
26.6.2 BER Display Page (SM, BHS) 344
26.6.3 Bridge Table Page (All) 345
26.6.4 Frame Calculator Page 345
26.6.5 Link Test Page (All) 349
26.6.6 Reg Failed SMs Page (AP, BHM) 350
26.6.7 Spectrum Analyzer Page (SM, BHS) 350

27 Maintaining Your Canopy Software 351
27.1 History of System Software Upgrades 351
27.1.1 System Release 3.1.5 Features 351
27.1.2 System Release 3.2 Features and Fixes 351
27.1.3 System Release 4.0 Features 351
27.1.4 System Release 4.0.1 Fixes 352
27.1.5 System Release 4.0.2 Fixes 352
27.1.6 System Release 4.0.4 Fix 352
27.1.7 System Release 4.1 Features 352
27.1.8 System Release 4.2.1 Features 353
27.1.9 System Release 4.2.2 Feature 353
27.1.10 System Release 4.2.3 Features and Fixes 353
27.1.11 System Release 4.2.7 Features and Fix 354
27.1.12 System Release 6.0 Features 354
27.1.13 System Release 6.1 Features and Fix 354

27.2 History of CMMmicro Software Upgrades 355
27.3 Typical Contents of Release Notes 355
27.4 Typical Upgrade Process 355
27.4.1 Downloading Software and Release Notes 355

28 Branding Web Pages 356
28.1 Rebranding web pages to Your Brand 356
28.2 Configuring a Hyperlinked Logo 358

29 Toggling Remote Access Capability 360
29.1 Denying All Remote Access 360
29.2 Reinstating Remote Access Capability 360

30 Setting Up a Protocol Analyzer on Your Canopy Network 362
30.1 Analyzing Traffic at an SM 362
30.2 Analyzing Traffic at an AP or BH with No CMM 363
30.3 Analyzing Traffic at an AP or BH with a CMM 363
30.4 Example of a Protocol Analyzer Setup for an SM 364

31 Troubleshooting 376
31.1 General Planning for Troubleshooting 376
31.2 General Fault Isolation Process 376
31.3 Questions to Help Isolate the Problem 377
31.4 Secondary Steps 377
31.5 Procedures for Troubleshooting 378
31.5.1 Module Has Lost or Does Not Establish Connectivity 378
31.5.2 NAT/DHCP-configured SM Has Lost or Does Not Establish Connectivity . 379
31.5.3 SM Does Not Register to an AP 380
31.5.4 BHS Does Not Register to a BHM 381
31.5.5 Module Has Lost or Does Not Gain Sync 381
31.5.6 Module Does Not Establish Ethernet Connectivity 382
31.5.7 Module Does Not Power Up 382
31.5.8 Power Supply Does Not Produce Power 383
31.5.9 CMM2 Does Not Power Up 384
31.5.10 CMM2 Does Not Pass Proper GPS Sync to Connected Modules 384
31.5.11 Module Software Cannot be Upgraded 385
31.5.12 Module Functions Properly, Except Web Interface Became Inaccessible .. 385

32 Obtaining Technical Support 386

33 Getting Warranty Assistance 391

CANOPY SYSTEM REFERENCE INFORMATION

34 Administering Modules through telnet Interface 393

35 Managing through a BAM Command-Line Interface 395

35.1 Caveats 395

35.2 SSE Database Commands 395

35.3 SSE telnet Commands 399

36 Legal and Regulatory Notices 400

36.1 Important Note on Modifications 400

36.2 National and Regional Regulatory Notices 400

36.2.1 U.S. Federal Communication Commission (FCC) and Industry Canada (IC) Notification 400

36.2.2 Regulatory Requirements for CEPT Member States (www.cept.org) 401

36.2.3 European Union Notification 402

36.2.4 UK Notification 402

36.2.5 Belgium Notification 403

36.2.6 Luxembourg Notification 403

36.2.7 Czech Republic Notification 403

36.2.8 Brazil Notification 403

36.2.9 Australia Notification 403

36.3 Exposure 403

36.4 Legal Notices 403

36.4.1 Software License Terms and Conditions 403

36.4.2 Hardware Warranty in U.S. 406

36.4.3 Limit of Liability 406

37 Additional Resources 407

38 History of Documentation 408

CANOPY SYSTEM WIRELESS AND BROADBAND TERMINOLOGY GLOSSARY

LIST OF FIGURES

Figure 1: Pole-mounted AP cluster 37
Figure 2: Structure-mounted SM 38
Figure 3: 900-MHz radio with flat panel antenna 38
Figure 4: Other flat panel antenna 38
Figure 5: Dish-mounted BH 39
Figure 6: 45-Mbps Backhaul Module ODU 40
Figure 7: 45-Mbps Backhaul Module PIDU 40
Figure 8: T1/E1 Multiplexer, front view 41
Figure 9: T1/E1 Multiplexer, rear view 41
Figure 10: CMM2 enclosure 42
Figure 11: CMM2 in pole-mounted system 42
Figure 12: Motorola GPS antenna 43
Figure 13: ACPS110 power supply 43
Figure 14: 27RD with mounted module 44
Figure 15: SMMB1 SM support bracket 44
Figure 16: 300SS surge suppressor 44
Figure 17: ACATHS-01 alignment headset 46
Figure 18: HSG-01 Housing 47
Figure 19: Part and serial numbers, exterior label 55
Figure 20: Part and serial numbers, interior label 55
Figure 21: ESN and model numbers, other interior label 58
Figure 22: Uplink data slot usage 61
Figure 23: TDD dividing Canopy frames 61
Figure 24: Uplink and downlink rate caps adjusted to apply aggregate cap 62
Figure 25: Uplink and downlink rate cap adjustment example 63
Figure 26: Canopy channel, 75% downlink, 0% high priority in uplink 65
Figure 27: Canopy channel, 75 % downlink, 40 % high priority (HP) uplink, software scheduling 65
Figure 28: Canopy channel, 75%downlink, 40% high priority (HP) in uplink, hardware scheduling 66
Figure 29: One unsynchronized AP in cluster 69
Figure 30: GPS timing throughout the Canopy network 70

Figure 31: Additional link to extend network sync, Design 3 71
Figure 32: Additional link to extend network sync, Design 4 71
Figure 33: Additional link to extend network sync, Design 5 72
Figure 34: Typical network layout with no BH 79
Figure 35: Typical network layout with BH 80
Figure 36: Typical multiple-BH network layout 80
Figure 37: Determinants in Rx signal level 97
Figure 38: Example layout of 7 Access Point clusters 106
Figure 39: Fresnel zone 109
Figure 40: Variables for calculating angle of elevation (and depression) 110
Figure 41: NAT Disabled implementation 118
Figure 42: NAT with DHCP Client and DHCP Server implementation 119
Figure 43: NAT with DHCP Client implementation 120
Figure 44: NAT with DHCP Server implementation 121
Figure 45: NAT without DHCP implementation 122
Figure 46: Example of IP address in Class B subnet 123
Figure 47: Canopy base cover, attached and detached 132
Figure 48: Canopy CMM2, bottom view 134
Figure 49: Cluster Management Module micro 135
Figure 50: Quick Start screen, AP 140
Figure 51: Time & Date screen, AP 142
Figure 52: Example Sessions page data, AP 144
Figure 53: LUID Select screen, AP 147
Figure 54: Status screen, SM 148
Figure 55: Status screen, AP 151
Figure 56: Quick Start screen, BHM 155
Figure 57: Time & Date screen, BHM 157
Figure 58: Example Sessions page data, BHM 159
Figure 59: LUID Select screen, BHM 162
Figure 60: Status screen, 5.2-GHz BHS 163
Figure 61: Status screen, BHM 166
Figure 62: CMMmicro layout 169
Figure 63: CMMmicro door label 171
Figure 64: CMMmicro circuit board 172
Figure 65: CMMmicro connections 173

Figure 66: Status screen, CMMmicro 174
Figure 67: Configuration screen, CMMmicro 177
Figure 68: GPS Status screen, CMMmicro 184
Figure 69: Port MIB screen, CMMmicro 185
Figure 70: Configuration screen (top), AP 189
Figure 71: Configuration parameters in 900-MHz AP 190
Figure 72: Configuration screen (middle), AP 195
Figure 73: Configuration screen (bottom), AP 201
Figure 74: IP Configuration screen, AP 204
Figure 75: Configuration screen, SM 207
Figure 76: Configuration screen, SM (continued) 211
Figure 77: IP Configuration screen, NAT disabled, public accessibility 215
Figure 78: IP Configuration screen, NAT disabled, local accessibility 216
Figure 79: IP Configuration screen, NAT with DHCP client and DHCP server 218
Figure 80: IP Configuration screen, NAT with DHCP client 219
Figure 81: IP Configuration screen, NAT with DHCP server 220
Figure 82: IP Configuration screen, NAT without DHCP 221
Figure 83: NAT Configuration screen, NAT disabled 223
Figure 84: Advanced Network Configuration screen of SM with NAT disabled 225
Figure 85: Advanced Network Configuration screen, NAT with DHCP client and DHCP server 227
Figure 86: NAT Configuration screen, NAT with DHCP client 228
Figure 87: NAT Configuration screen, NAT with DHCP server 229
Figure 88: NAT Configuration screen, NAT without DHCP 230
Figure 89: VLAN Configuration screen, SM 233
Figure 90: Configuration screen, BHM 236
Figure 91: Configuration screen, BHM (continued) 240
Figure 92: IP Configuration screen, BHM 244
Figure 93: Configuration screen, BHS 246
Figure 94: Configuration screen, BHS (continued) 250
Figure 95: IP Configuration screen, BHS 254
Figure 96: Signal information screen for PDA access, Release 4.2 258
Figure 97: AP Evaluation screen for PDA access, Release 4.2 258
Figure 98: Module information screen for PDA access, Release 4.2 259
Figure 99: Detail of GPS antenna mounting 261

Figure 100: Detail of pole mounting 263
Figure 101: Location of 115-/230-volt switch 264
Figure 102: Layout of logical connections in CMM2 265
Figure 103: Canopy CMM2, front view 266
Figure 104: Port indicator LED on Ethernet switch 267
Figure 105: SM attachment to reflector arm 272
Figure 106: SM and computer wiring 272
Figure 107: Audible Alignment Tone kit and example tone 274
Figure 108: Correct mount, with module support arm plumb behind reflector dish 276
Figure 109: Incorrect mount, with module plumb in front of reflector dish 276
Figure 110: Mounting assembly, exploded view 277
Figure 111: BH attachment to reflector arm 278
Figure 112: Alignment screen 280
Figure 113: Audible Alignment Tone kit and example tone 281
Figure 114: Spectrum Analyzer screen, 900-MHz SM 286
Figure 115: Spectrum Analyzer screen, 2.4-GHz SM 288
Figure 116: Example of private IP network 295
Figure 117: Categorical protocol filtering 304
Figure 118: Example block of Event Log page data 331
Figure 119: Example AP Eval Data screen 333
Figure 120: Example Sessions page data 335
Figure 121: GPS Status screen 337
Figure 122: Status screen, AP, after Expanded Stats is selected 340
Figure 123: Status Screen, SM, after Expanded Stats is selected 341
Figure 124: BER Results screen 344
Figure 125: Bridge Table screen 345
Figure 126: Discovering downlink data percentages for collocation 347
Figure 127: Discovering downlink data percentages for collocation, continued 348
Figure 128: Link Test screen 349
Figure 129: Reg Failed SMs screen 350
Figure 130: Example ftp session to transfer logo 356
Figure 131: Example telnet session to change screen logo 357
Figure 132: Example ftp session to transfer logo and hyperlink file 358
Figure 133: Example telnet session to add logo and hyperlink file 359
Figure 134: Protocol analysis at SM 362

Figure 135: Protocol analysis at AP or BH not connected to a CMM 363
Figure 136: Protocol analysis at AP or BH connected to a CMM 364
Figure 137: IP Configuration screen for SM 365
Figure 138: Local Area Connection menu 366
Figure 139: Local Area Connection Properties window 367
Figure 140: Internet Protocol (TCP/IP) Properties window 368
Figure 141: Status screen for SM 369
Figure 142: Ethereal software launch window 370
Figure 143: Capture menu 371
Figure 144: Ethereal Capture Options window 372
Figure 145: Ethereal Capture window 373
Figure 146: <capture> - Ethereal window, Packet 1 selected 374
Figure 147: <capture> - Ethereal window, Packet 14 selected 375

LIST OF TABLES

Table 1: Canopy User Guide organization scheme 27
Table 2: Examples of where to find information in this user guide 28
Table 3: Locations of screen captures and associated documentation 29
Table 4: Font types 31
Table 5: Admonition types 31
Table 6: Essential user guide elements for new backhaul network implementation 35
Table 7: Recommended outdoor UTP Category 5E cables 45
Table 8: Recommended indoor UTP Category 5E cables 45
Table 9: Recommended antenna cables 46
Table 10: Product applications per frequency band range 48
Table 11: Range, throughput, and encryption per frequency band range, PTMP links 49
Table 12: Range, throughput, and encryption per frequency band range, PTP links 49
Table 13: Cluster management product similarities and differences 50
Table 14: CMM2 specifications and limitations 53
Table 15: CMMmicro specifications and limitations 54
Table 16: Differences between software and hardware scheduling 67
Table 17: Downlink and uplink PTMP throughput, 2-mile link, software scheduling 74
Table 18: Downlink and uplink PTMP throughput, 15-mile link, software scheduling 75
Table 19: Effects of network conditions on PTMP throughput 76
Table 20: Canopy features and their benefits 82
Table 21: Demonstration Kit part numbers 91
Table 22: Starter Kit Part Numbers 93
Table 23: Example 900-MHz channel assignment by sector 104
Table 24: Example 2.4-GHz channel assignment by sector 105
Table 25: Example 5.2-GHz channel assignment by sector 105
Table 26: Example 5.4-GHz channel assignment by sector 105
Table 27: Example 5.7-GHz channel assignment by sector 106
Table 28: Range of links with and without Passive Reflector 111
Table 29: Range of 2.4-GHz BH with and without Passive Reflector 112
Table 30: Range of 5.2-GHz BH with and without Passive Reflector 112
Table 31: Range of 5.4-GHz BH with and without Passive Reflector 113
Table 32: Range of 5.7-GHz BH with and without Passive Reflector 113

Table 33: Exposure separation distances 127
Table 34: Power Compliance Margins 128
Table 35: LEDs in AP and BHM 133
Table 36: LEDs in SM and BHS 133
Table 37: Cable scheme auto-sensing per MAC address 136
Table 38: Port Configuration selections for CMMmicro 179
Table 39: When Changes Become Effective in CMMmicro 183
Table 40: Slot settings for all APs in cluster, based on traffic type 192
Table 41: Control slot settings for all APs in cluster with Hardware Scheduler 192
Table 42: Where feature values are obtained for the SM with authentication required .. 235
Table 43: Where feature values are obtained for the SM with authentication disabled .. 235
Table 44: Patch antenna and reflector gain 256
Table 45: Differences between graphical and tabular Spectrum Analyzer page 286
Table 46: Hardware series by MAC address 289
Table 47: FPGA and CANOPYBOOT versions 290
Table 48: Upgradability from previous software releases 291
Table 49: Compatibility of software releases 292
Table 50: AP/BH compatibility with CMMmicro 293
Table 51: Types of access per password combination 298
Table 52: Ports filtered per protocol selections 305
Table 53: Examples of SM tiers 307
Table 54: Categories of MIB-II objects 310
Table 55: Canopy Enterprise MIB objects for APs, SMs, and BHs 313
Table 56: Canopy Enterprise MIB objects for APs and BH timing masters 314
Table 57: Canopy Enterprise MIB objects for SMs and BH timing slaves 318
Table 58: Canopy Enterprise MIB objects for CMMmicros 321
Table 59: Canopy 45-Mbps BH module MIB objects 324
Table 60: Event Log messages for abnormal events 332
Table 61: Event Log messages for normal events 332
Table 62: Basic site information for technical support 387
Table 63: Supported telnet commands for module administration 393
Table 64: US FCC IDs and Industry Canada Certification Numbers 401

LIST OF PROCEDURES

Procedure 1: Modifying a fixed license key for a module IP address 86
Procedure 2: Analyzing the spectrum 98
Procedure 3: Invoking the low power mode 114
Procedure 4: Wrapping the cable 130
Procedure 5: Setting up the AP for Quick Start 138
Procedure 6: Bypassing proxy settings to access module web pages 139
Procedure 7: Using Quick Start to configure the AP for test 141
Procedure 8: Setting up the SM for test 143
Procedure 9: Retrying to establish a point-to-multipoint link 144
Procedure 10: Viewing SM pages through the AP 147
Procedure 11: Verifying and recording information from SMs 150
Procedure 12: Verifying and recording information from the AP 153
Procedure 13: Setting up the BH for Quick Start 153
Procedure 14: Using Quick Start to configure the BH for test 155
Procedure 15: Setting up the BHS for test 158
Procedure 16: Retrying to establish a point-to-point link 159
Procedure 17: Viewing BHS pages through the BHM 162
Procedure 18: Viewing BHS pages through the BHM 163
Procedure 19: Verifying and recording information from the BHS 166
Procedure 20: Verifying and recording information from the BHM 168
Procedure 21: Configuring a CMMmicro 170
Procedure 22: Setting CMMmicro parameters for test 178
Procedure 23: Installing the AP 259
Procedure 24: Mounting the GPS antenna 261
Procedure 25: Mounting the CMM2 262
Procedure 26: Cabling the CMM2 263
Procedure 27: Verifying CMM2 Connections 267
Procedure 28: Mounting the CMMmicro 268
Procedure 29: Installing the Power Supply for the CMMmicro 269
Procedure 30: Cabling the CMMmicro 270
Procedure 31: Verifying CMMmicro Connections 271
Procedure 32: Installing the SM 271

Procedure 33: Verifying system performance 275
Procedure 34: Installing the BHM 277
Procedure 35: Installing the BHS 279
Procedure 36: Verifying performance for a BH link 282
Procedure 37: Verifying System Functionality 283
Procedure 38: Using the Spectrum Analyzer in AP feature 289
Procedure 39: Extending network sync 294
Procedure 40: Fabricating an override plug 300
Procedure 41: Regaining access to a module 301
Procedure 42: Using the override switch to regain access to CMMmicro 302
Procedure 43: Installing the Canopy Enterprise MIB files 311
Procedure 44: Replacing the Canopy logo 356
Procedure 45: Changing the hyperlinked URL for the top of Canopy web pages 358
Procedure 46: Denying all remote access 360
Procedure 47: Reinstating remote access capability 360
Procedure 48: Troubleshooting loss of connectivity 378
Procedure 49: Troubleshooting loss of connectivity for NAT/DHCP-configured SM 379
Procedure 50: Troubleshooting SM failing to register to an AP 380
Procedure 51: Troubleshooting BHS failing to register to a BHM 381
Procedure 52: Troubleshooting loss of sync 381
Procedure 53: Troubleshooting loss of Ethernet connectivity 382
Procedure 54: Troubleshooting failure to power up 382
Procedure 55: Troubleshooting failure of power supply to produce power 383
Procedure 56: Troubleshooting CMM2 that malfunctions 384
Procedure 57: Troubleshooting CMM2 not passing sync 384
Procedure 58: Troubleshooting an unsuccessful software upgrade 385
Procedure 59: Restoring the web interface to a module 385

GUIDE TO THIS USER GUIDE

1 NEW IN THIS ISSUE

In Issue 1 of this user guide, this section is a placeholder where changes will be listed in future issues.

1.1 PRODUCTS COVERED BY THIS USER GUIDE

Most Canopy products are covered by this user guide:

- 900-MHz AP and SM
- 2.4-GHz modules
- 5.2-GHz modules
- 5.4-GHz modules
- 5.7-GHz modules
- Cluster Management Module 2 (CMM2)
- Cluster Management Module micro (CMMmicro)
- Surge Suppressor

1.2 PRODUCTS NOT COVERED BY THIS USER GUIDE

Some specific-use Canopy products are briefly described in this user guide but fully described in their own separate user guides:

- 45-Mbps Backhaul Module. See *Canopy 45-Mbps Backhaul User Guide*.
- Bandwidth and Authentication Manager. See *Canopy Bandwidth and Authentication Manager (BAM) User Guide*.
- License Manager. See *Canopy Networks License Manager User Guide*.
- T1/E1 Multiplexer. See *Canopy T1/E1 Multiplexer User Guide*.

1.3 SOFTWARE COMPATIBILITY DESCRIBED IN THIS USER GUIDE

The following sections of this document provide details and caveats about the compatibility of Canopy products:

- Designations on Page 289
- Application, Boot, and FPGA Software Upgrades on Page 290
- System Release 6.1 Compatibility on Page 291
- BAM Software Compatibility on Page 292
- CMMmicro Software and Hardware Compatibility on Page 293
- MIB File Set Compatibility on Page 293

2 USING THIS USER GUIDE

This document should be used with Canopy features through Software Release 6.1 and CMMmicro Release 2.1.1. The audience for this document includes system operators, network administrators, and equipment installers.

2.1 FINDING THE INFORMATION YOU NEED

Previous publications of Canopy user documentation were organized by the type of equipment. Logically then, each was a user manual about a module. The user *manual* format had many redundancies and deficiencies that the user *guide* format avoids.

The user guide format

- provides more and better information about how Canopy modules interact with each other, in both communications and compatibility.
- organizes information by the task that the information supports (and thus, in many cases, by the role that the user plays in the client company).
- suggests when information from Canopy module web pages or an SNMP network management station should be watched carefully, used, or ignored.
- defines what the important Canopy system messages and field values mean.

2.1.1 Becoming Familiar with This User Guide

This is a guide to the guide. A high-level overview of the guide and some examples of where to look provide insight into how information is arranged and labeled.

The Table of Contents provides not only a sequential index of topics but also a visual glance at the organization of topics in this guide. A few minutes spent with the Table of Contents in either the paper or the electronic version of this guide can save much more time in finding information now and in the future. The List of Procedures may be especially useful in the paper version of this guide, particularly where you mark those procedures that you wish to frequently see.

In contrast, the List of Figures and List of Tables are most useful for automated searches on key words in the electronic version of this guide. If a match is present, the match is the first instance that the search finds.

Quick Reference

The Canopy User Guide comprises six sections, as described in Table 1.

Table 1: Canopy User Guide organization scheme

Section	Purpose
Guide to This User Guide (this section)	Identifies ◦ products covered by this user guide. ◦ products covered by their own separate user guides. ◦ how this user guide is organized. ◦ where to find module web pages and parameter descriptions. ◦ what the various typefaces and admonitions indicate. ◦ how to contact Canopy.
Understanding Canopy Networks	Provides ◦ references to RF and networking theory. ◦ a list of sections to see if you are building only a backhaul network. ◦ overviews and comparisons of Canopy products and how they communicate. ◦ descriptions of data handling and synchronization. ◦ a review of Canopy optional features. ◦ resources for developing familiarity and proficiencies with Canopy networks.
Designing Your Canopy Network	Provides essential information for ◦ evaluating an area for a Canopy network. ◦ specifying the IP addresses and frequency band ranges to use for each type of link.
Building Your Canopy Network	Provides systematic approaches for ◦ avoiding hazards from RF and natural causes. ◦ testing, storing, and deploying Canopy equipment.
Managing Your Canopy Network	Provides guidance for ◦ expanding network coverage. ◦ improving the security of Canopy wireless links. ◦ distributing bandwidth resources. ◦ monitoring and changing variables through SNMP.
Canopy System Reference Information	Provides supplemental information such as ◦ authorizations, approvals, and notices. ◦ a bibliography of adjunctive information sources. ◦ a history of changes in Canopy documentation.
Canopy System and Wireless Broadband Terminology Glossary	Defines terms and concepts that are used in this user guide.

Examples

A list of common tasks and references to information that supports each task is provided in Table 2.

Table 2: Examples of where to find information in this user guide

If you want to know…	then see…	because…
what the Spectrum Analyzer in SM and BHS feature does	Avoiding Self Interference on Page 114	this topic is important to RF planning.
	Monitoring the RF Environment on Page 285	this topic is also important to managing the network.
what software releases support the Spectrum Analyzer in SM and BHS feature.	System Release 4.1 Features on Page 352	this section is where the feature sets are distinguished by release.
what types of slots compose the Canopy frame	Understanding Bandwidth Management on Page 59	this information is helpful for understanding Canopy networks.
how to set the acknowledgement and control slot parameters	Slot Specifications on Page 192	setting these parameters is part of configuring an AP for its destination.
how to calculate whether an object will interfere with a signal	Noting Possible Obstructions in the Fresnel Zone on Page 99	this topic is important to RF planning.
how long a cable you can use from the GPS antenna to the CMM	Cables on Page 26	cables are accessory components.
	Procedure 24 on Page 261 *or* Procedure 28 on Page 268	the advisory applies to mounting GPS antennas *and* CMMs.
how to react to a WatchDog Event Log message	Messages that Flag Abnormal Events on Page 332 *and* Messages that Flag Normal Events on Page 332	together, these two sections document all significant Event Log messages.
what beam angle the passive reflector dish produces	Specifications and Limitations on Page 52, then downward to a table for a Canopy Part Number that includes “RF.”	the beam angle is a specification.
how to aim the passive reflector dish	Installing a Reflector Dish on Page 275	aiming is associated with Backhaul Module installation.

2.1.2 Searching This User Guide

To search this document and the software release notes of supported releases, look

- in the Table of Contents for the topic.
- in the Adobe Reader® search capability for keywords that apply.[1]

2.1.3 Finding Parameter and Field Definitions for Module Web Pages

Because this user guide is sequentially arranged to support tasks, and various tasks require different settings and readings, parameter and field definitions are scattered according to the tasks that they support. The locations of these are provided in Table 3.

Table 3: Locations of screen captures and associated documentation

Module Web Page Screen Capture	Page
Advanced Network Configuration screen of SM with NAT disabled	225
Advanced Network Configuration screen, NAT with DHCP client and DHCP server	227
Alignment screen	280
AP Evaluation screen for PDA access, Release 4.2	258
BER Results screen	344
Bridge Table screen	345
Configuration parameters in 900-MHz AP	190
Configuration screen, 5.2-GHz SM	207
Configuration screen, AP	189
Configuration screen, AP (continued)	195
Configuration screen, BHM	236
Configuration screen, BHM (continued)	240
Configuration screen, BHS	246
Configuration screen, BHS (continued)	250
Configuration screen, CMMmicro	177
Configuration screen, SM (continued)	211
Example AP Eval Data screen	333
Example block of Event Log page data	331
Example Sessions page data	335
Example Sessions page data, AP	144
Example Sessions page data, BHM	159

[1] Reader is a registered trademark of Adobe Systems, Incorporated.

Module Web Page Screen Capture	Page
GPS Status screen	337
GPS Status screen, CMMmicro	184
IP Configuration screen for SM	365
IP Configuration screen, AP	204
IP Configuration screen, BHM	244
IP Configuration screen, BHS	254
IP Configuration screen, NAT disabled, local accessibility	216
IP Configuration screen, NAT disabled, public accessibility	215
IP Configuration screen, NAT with DHCP client	219
IP Configuration screen, NAT with DHCP client and DHCP server	218
IP Configuration screen, NAT with DHCP server	220
IP Configuration screen, NAT without DHCP	221
Link Test screen	349
LUID Select screen, AP	147
LUID Select screen, BHM	162
Module information screen for PDA access, Release 4.2	259
NAT Configuration screen, NAT disabled	223
NAT Configuration screen, NAT with DHCP client	228
NAT Configuration screen, NAT with DHCP server	229
NAT Configuration screen, NAT without DHCP	230
Port MIB screen, CMMmicro	185
Quick Start screen, AP	140
Quick Start screen, BHM	155
Reg Failed SMs screen	350
Signal information screen for PDA access, Release 4.2	258
Spectrum Analyzer screen, 2.4-GHz SM	288
Spectrum Analyzer screen, 900-MHz SM	286
Status screen for SM	369
Status screen, 2.4-GHz SM	148
Status screen, 5.2-GHz BHS	163
Status screen, AP	151
Status screen, BHM	166
Status screen, CMMmicro	174

Module Web Page Screen Capture	Page
Time & Date screen, AP	142
Time & Date screen, BHM	157

2.2 INTERPRETING TYPEFACE AND OTHER CONVENTIONS

This document employs distinctive fonts to indicate the type of information, as described in Table 4.

Table 4: Font types

Font	Type of Information
variable width bold	Selectable option in a graphical user interface or settable parameter in the web-based interface to a Canopy component.
`constant width regular`	Literal system response in a command-line interface.
`constant width italic`	Variable system response in a command-line interface.
`constant width bold`	Literal user input in a command-line interface.
`constant width bold italic`	Variable user input in a command-line interface.

This document employs specific imperative terminology as follows:

- *Type* means press the following characters.
- *Enter* means type the following characters and then press Enter.

This document also employs a set of consistently used admonitions. Each of these types of admonitions has a general purpose that underlies the specific information in the box. These purposes are indicated in Table 5.

Table 5: Admonition types

Admonition Label	General Message
	NOTE: informative content that may ◦ defy common or cursory logic. ◦ describe a peculiarity of the Canopy implementation. ◦ add a conditional caveat. ◦ provide a reference. ◦ explain the reason for a preceding statement or provide prerequisite background for what immediately follows.

Admonition Label	General Message
	RECOMMENDATION: suggestion for an easier, quicker, or safer action or practice.
	IMPORTANT! informative content that may ◦ identify an indication that you should watch for. ◦ advise that your action can disturb something that you may not want disturbed. ◦ reiterate something that you presumably know but should always remember.
	CAUTION! a notice that the risk of harm to equipment or service exists.
	WARNING! a notice that the risk of harm to person exists.

2.3 GETTING ADDITIONAL HELP

Help is available for problems with supported products and features. Obtaining Technical Support on Page 386 provides the sequence of actions that you should take if these problems arise.

2.4 SENDING FEEDBACK

We welcome your feedback on Canopy system documentation. This includes feedback on the structure, content, accuracy, or completeness of our documents, and any other comments you have. Send your comments to technical-documentation@canopywireless.com.

UNDERSTANDING CANOPY NETWORKS

3 ADVANCING FROM RESEARCH TO IMPLEMENTATION

Before you begin to research a possible Canopy implementation, you should have both

- basic knowledge of RF theory. See
  - Understanding RF Fundamentals on Page 88.
  - Engineering Your RF Communications on Page 96.
- network experience. See
  - Canopy Link Characteristics on Page 59.
  - Understanding IP Fundamentals on Page 88.
  - Engineering Your IP Communications on Page 116.

4 REALIZING A WIRELESS BACKHAUL NETWORK

To establish and maintain a Canopy wireless backhaul network, you should be familiar with the elements of this user guide that are listed in Table 6.

Table 6: Essential user guide elements for new backhaul network implementation

Element	Title	Page
Section 5.1.5	Backhaul Module	39
Section 5.1.6	45-Mbps Backhaul Module	39
Section 5.1.8	T1/E1 Multiplexer	41
Section 5.1.9	Cluster Management Module 2 (Part 1008CK)	42
Section 5.1.10	Cluster Management Module micro (Part 1070CK)	42
Section 8.2	BH-BH Links	76
Figure 36	Typical multiple-BH network layout	80
Section 12.2	Analyzing the RF Environment	98
Section 12.3	Considering Frequency Band	100
Section 15	Avoiding Hazards	127
Section 16.4	Configuring a Point-to-Point Link for Test	153
Section 17	Preparing Components for Deployment	187
Section 18.4	Configuring a BH Timing Master for the Destination	235
Section 18.5	Configuring a BH Timing Slave for the Destination	246
Section 19.4	Installing a GPS Antenna	260
Section 19.5	Installing a CMM2	262
Section 19.6	Installing a CMMmicro	268
Section 19.9	Installing a Reflector Dish	275
Section 19.10	Installing a BH Timing Master	277
Section 19.11	Installing a BH Timing Slave	279
Section 19.13	Verifying a BH Link	282
Section 20	Verifying System Functionality	283
Section 21.2.5	CMMmicro Software and Hardware Compatibility	293
Section 22.2	Encrypting Canopy Radio Transmissions	296
Section 22.3	Managing Password Access	297
Section 25	Interpreting Data in the GPS Status Page (AP, BHM)	327
Section 27.3	Typical Contents of Release Notes	355
Section 27.4	Typical Upgrade Process	355
Section 29	Toggling Remote Access Capability	360

Section 30.2	Analyzing Traffic at an AP or BH with No CMM	363
Section 30.3	Analyzing Traffic at an AP or BH with a CMM	363
Section 31	Troubleshooting	376
Section 32	Obtaining Technical Support	386
Section 33	Getting Warranty	391

5 EXPLORING THE SCOPE OF SOLUTIONS

Canopy wireless broadband applications include:

- local area network (LAN) extensions
- Internet subscriber service
- high-bandwidth point-to-point connections
- multicast video (for instruction or training, for example)
- private branch exchange (PBX) extensions
- point-to-multipoint data backhaul
- redundant network backup
- video surveillance
- voice over IP (VoIP)
- TDM over Ethernet (for legacy voice and data)

5.1 COMPONENTS

Canopy networks use some or all of the following components.

5.1.1 Access Point Module

The Access Point Module (AP) distributes network or Internet services in a 60° sector to 200 subscribers or fewer (and not more than 4,096 MAC addresses, which may be directly-connected PCs, IP appliances, gateways, SMs, and the AP, except that *no limit* applies behind subscriber NAT gateways). The AP is configurable through a web interface.

5.1.2 Access Point Cluster

The AP cluster consists of two to six APs that together distribute network or Internet services to a community of 1,200 or fewer subscribers. Each AP transmits and receives in a 60° sector. An AP cluster covers as much as 360°.

An AP cluster is pictured in Figure 1.

Figure 1: Pole-mounted AP cluster

5.1.3 Subscriber Module

The Subscriber Module (SM) is a customer premises equipment (CPE) device that extends network or Internet services by communication with an AP. The SM is configurable through a web interface.

An SM mounted directly to a structure is pictured in Figure 2.

Figure 2: Structure-mounted SM

5.1.4 900-MHz AP and SM

Canopy 900 MHz AP and SM modules operate at 3.3 Mbps (compared to 10 Mbps for other Canopy frequency bands). With Downlink Data set to 75% on the AP Configuration page, the AP supports high throughput to an SM.

These 900-MHz modules run the same software and provide the same parameters, network features, and connections as all other Canopy APs and SMs. The physics of longer-wavelength 900 MHz, the power allowed by regulatory authorities, and the low Canopy Carrier-to-Interference (C/I) ratio combine to support:

- LOS range of 40 miles (over 64 km)
- increased NLOS range, depending on RF considerations such as foliage, topography, and obstructions.

Figure 3: 900-MHz radio with flat panel antenna

When collocated with a Canopy SM of another frequency band range, the 900-MHz AP may serve, without a tower or BH, as a *remote* AP. The SM provides the Spectrum Analyzer feature.

900-MHz modules operate on only the unique Canopy System Release 4.2.2 or later releases, but can be used in networks that also consist of modules in other frequency bands operating on earlier Canopy system releases.

Figure 4: Other flat panel antenna

For example, 900-MHz APs and SMs are logical choices for extending Canopy 2.4-, 5.2-, and 5.7-GHz radio networks where you wish to

- add subscriber-handling capacity to a tower that is either
  - fully used in the other frequency band ranges.
  - not available to any other frequency band range.
- reach sparsely populated areas.
- penetrate foliage.
- add a remote AP behind an SM that operates in another frequency band range.

5.1.5 Backhaul Module

The Backhaul Module (BH) provides point-to-point connectivity in either

- a standalone RF or wired link to another BH
- a wired link through a cluster management module to an AP cluster.

You must configure a BH as either a timing master (BHM) or timing slave (BHS). The BHM provides sync to the BHS.

A BH mounted to a passive reflector dish is pictured in Figure 5.

Figure 5: Dish-mounted BH

5.1.6 45-Mbps Backhaul Module

The 45-Mbps BH provides point-to-point data connectivity via a 5.8-GHz wireless Ethernet bridge that operates at broadband data rates. The 45 Mbps Backhaul serves enterprises that need to connect the Local Area Networks (LANs) of two or more buildings.

The 45-Mbps BH provides non-Line of Sight (NLOS) operation through the use of both Orthogonal Frequency Division Multiplex (OFDM) modulation and Multi-Beam Space Time Coding (STC). Transmissions penetrate foliage and such that almost universal coverage is typical at short range.

The 45-Mbps BH link consists of a pair of identical BHs that transmit and receive on an automatically selected but configurable frequency. The installer sets up one unit as the master and the other as the slave. (Each unit is preconfigured

as master or slave but can be reconfigured to the other.) Each end of the link consists of both

- an integrated outdoor transceiver (ODU) that contains all the radio and networking electronics.
- an indoor passive connection box (PIDU) that contains status indicators and network connection.

Figure 6: 45-Mbps Backhaul Module ODU

Carrier applications for the 45-Mbps BH include reaching remote AP clusters, interconnecting campus buildings or remote branch offices, extending PBX circuits, backhauling cell sites, and extending central office T1s/E1s.

The 45-Mbps BH uses a proprietary data scrambling and encryption scheme. AES encryption is available as an option.

This product is supported by the dedicated document *Canopy 45-Mbps Backhaul User Guide*.

5.1.7 Power Indoor Unit for 45-Mbps Backhaul Module

The 45-Mbps Backhaul Module PIDU generates the voltage for the ODU. The PIDU also provides status indicators for the ODU (over the blue and blue/white pair that are connected to Pins 4 and 5 of the RJ-45 plugs and jacks.)

Figure 7: 45-Mbps Backhaul Module PIDU

5.1.8 T1/E1 Multiplexer

The Canopy T1/E1 Multiplexer converts the data stream from T1/E1 ports into Ethernet packets that are then transported over the Canopy BH link. This enables up to four T1 (or up to three E1) circuits to be extended over Ethernet networks. The T1/E1 Multiplexer is available in two power configurations:

- an external 3.3-v DC power source from a 120/240-v AC adapter (supplied by Canopy)
- an optional connection to an external −48 v DC supply for battery backup.

Figure 8: T1/E1 Multiplexer, front view

The T1/E1 Multiplexer supports

- synchronous TDM-based services over wireless Ethernet networks.
- CAS signaling transparent to all other signaling protocols on T1/E1.
- 10Base-T/100Base-TX uplink to the network.
- management interfaces.
- simplified troubleshooting through T1/E1 line loopback test.

Figure 9: T1/E1 Multiplexer, rear view

Applications include

- obviating leased lines.
- implementing wireless PBX networking.
- establishing cellular backhaul links.
- providing homeland security backup or emergency voice networks.
- routing LAN/WAN data on excess bandwidth.

This product is supported by the dedicated document *Canopy T1/E1 Multiplexer User Guide*.

5.1.9 Cluster Management Module 2 (Part 1008CK)

The Cluster Management Module 2 (CMM2) provides power, GPS timing, and networking connections for an AP cluster. If the CMM2 is also connected to a BH, then the CMM2 is the central point of connectivity for the entire site. The CMM2 can connect as many as eight collocated modules—APs, BHMs, BHSs—and an Ethernet feed.

The CMM2 requires two cables for each connected module:

- One provides Ethernet communications and power. This cable terminates in an RJ-45 connector.
- The other provides synchronization (sync), GPS status, and time and date in a serial interface. This cable terminates in an RJ-11 connector.

A CMM2 is pictured in Figure 10. A CMM2 as part of a mounted Canopy system is pictured in Figure 11.

Figure 10: CMM2 enclosure

Figure 11: CMM2 in pole-mounted system

5.1.10 Cluster Management Module micro (Part 1070CK)

The Cluster Management Module micro (CMMmicro) provides power, GPS timing, and networking connections for an AP cluster. If the CMMmicro is connected to both an AP cluster and a BH, then the CMMmicro is the central point of connectivity for the entire site. Unlike the CMM2, the CMMmicro is configurable through a web interface.

The CMMmicro contains an 8-port managed switch that supports Power over Ethernet (PoE) on each port and connects as many as eight collocated modules—APs, BHMs, BHSs—and an Ethernet feed. The CMMmicro auto-negotiates speed to match inputs that are either 100Base-TX or 10Base-T, and either full duplex or half duplex. Alternatively, these parameters are settable.

A CMMmicro requires only one cable, terminating in an RJ-45 connector, for each connected module to distribute

- Ethernet signaling.
- power to as many as 8 collocated modules—APs, BHMs, or BHSs. Through a browser interface to the managed switch, ports can be powered or not.

- sync to APs and BHMs. The CMMmicro receives 1-pulse per second timing information from Global Positioning System (GPS) satellites through an antenna and passes the timing pulse in 24-V power to the connected modules.

GPS status information is available at the CMMmicro, which *does not* pass this information to connected BHMs or APs, with the following exception:

- CMMmicro *does not* provide time and date information to BHMs and APs if either the CMMmicro is operating on a release earlier than CMMmicro Release 2.1 or the AP/BHM is operating on a release earlier than Canopy System Release 4.2.
- CMMmicro provides time and date information to BHMs and APs if both the CMMmicro is operating on CMMmicro Release 2.1 or later release and the AP/BHM is operating on Canopy System Release 4.2 or later release.
See Time & Date Page of the AP on Page 141.

5.1.11 Accessory Components

In addition to the above modules, the following accessories are available.

GPS Antenna

The Motorola GPS antenna provides either

- timing pulses to the CMMmicro.
- timing pulses and positioning information to the CMM2.

The GPS antenna is pictured in Figure 12.

Figure 12: Motorola GPS antenna

Power Supplies

The 110-V AC input Motorola ACPS110-03 power supply provides 24-V/400-mA power to SMs in Canopy networks in U.S.A., NOM, and Canada. The ACPS110-03 is pictured in Figure 13.

The 100- to 240-V AC input Motorola ACPS100-01 power supply provides 50- to 60-Hz 100-W power to the CMMmicro.

100- to 240-V AC input variations of the above are available as

- the Motorola ACPSSW-02 power supply, which includes a Europlug (CEE 7/16) adaptor.
- the Motorola ACPSSW-03 power supply, which includes an Argentina adaptor.
- the Motorola ACPSSW-04 power supply, which includes an Australia adaptor.
- the Motorola ACPSSW-04 power supply,

Figure 13: ACPS110 power supply

which includes a China adaptor.

Passive Reflector Dish Assembly

The 27RD Passive Reflector Dish extends the distance range of a module and focuses the beam into a narrower angle. The internal patch antenna of the module illuminates the Canopy Passive Reflector Dish from an offset position. The module support tube provides the proper angle for this offset.

A 27RD with a module mounted is pictured in Figure 14.

Figure 14: 27RD with mounted module

Subscriber Module Support Bracket

The SMMB1 support bracket facilitates mounting the SM to various surfaces of a structure and has slots through which chimney straps can be inserted. An SMMB1 is pictured in Figure 15.

Figure 15: SMMB1 SM support bracket

Surge Suppressor

The 300SS Surge Suppressor provides a path to ground (Protective Earth) that protects connected subscriber home equipment from near-miss lightning strikes. A 300SS is pictured in Figure 16.

Figure 16: 300SS surge suppressor

Cables

Canopy modules that are currently or recently sold can auto-sense whether the Ethernet cable is wired as straight-through or crossover. Some modules that were sold earlier cannot. The MAC address, visible on the module, distinguishes whether the module can. See Table 37 on Page 136. All CMMmicros can auto-sense the cable scheme.

Where a non auto-sensing module is deployed

- a straight-through cable must be used for connection to a network interface card (NIC).
- a crossover cable must be used for connection to a hub, switch, or router.

Canopy-recommended Ethernet and sync cables can be ordered in lengths up to 328 ft (100 m) from Best-Tronics Manufacturing, Inc. at http://www.best-tronics.com/motorola.htm. These cables are listed in Table 7 and Table 8.

Table 7: Recommended outdoor UTP Category 5E cables

Part #	Description
BT-0562	RJ-45 TO RJ-45; straight-through Ethernet cable
BT-0562S	RJ-45 TO RJ-45; shielded straight-through Ethernet cable
BT-0565	RJ-45 TO RJ-45; crossover Ethernet cable
BT-0565S	RJ-45 TO RJ-45; shielded crossover Ethernet cable
BT-0563	RJ-11 TO RJ-11; sync cable
BT-0563S	RJ-11 TO RJ-11; shielded sync cable

NOTE:
Shielded cable is strongly recommended for all AP cluster and BH installations.

Table 8: Recommended indoor UTP Category 5E cables

Part #	Description
BT-0596	RJ-45 TO RJ-45; straight-through Ethernet cable
BT-0595	RJ-45 TO RJ-45; crossover Ethernet cable

Approved Ethernet cables can also be ordered as bulk cable:

- CA-0287
- CA-0287S (shielded)

Canopy-approved antenna cables can be ordered in lengths up to 100 ft (30.4 m), as listed in Table 9.

Table 9: Recommended antenna cables

Part #	Description
BT-0564	N TO N GPS antenna cable for CMM2
BT-0716	BNC TO N GPS antenna cable for CMMmicro

Category 5 Cable Tester

For purchase within the U.S.A., the CTCAT5-01 Cable Tester is available.

Override Plug

An override plug (sometimes called a default plug) is available to provide access to a module whose password and/or IP address have been forgotten. This plug allows the AP, SM, or BH to be accessed using IP address 169.254.1.1 and no password. During the override session, you can assign any new IP address and set either or both user passwords (display-only and/or full access) as well as make other parameter changes.

This plug is available from Best-Tronics Manufacturing, Inc. at http://www.best-tronics.com/motorola.htm as Part BT-0583 (RJ-11 Default Plug). Alternatively if you wish, you can fabricate an override plug, using instructions provided in Procedure 40 on Page 300.

Alignment Headset

The ACATHS-01 Alignment Headset facilitates the operation of precisely aiming an SM toward an AP (or a BHS toward a BHM). This device produces infinitely variable

- pitch, higher when the received signal is stronger.
- volume, louder when jitter is less.

An ACATHS-01 is pictured in Figure 17.

Figure 17: ACATHS-01 alignment headset

Module Housing

The HSG-01 Canopy Plastic Housing is available for replacement of a damaged housing on a module that is otherwise functional. The HSG-01 is pictured in Figure 18.

The HSG-01 and all module housings of this design provide clearances for cable ties on the Ethernet and sync cables.

> *RECOMMENDATION:*
> Use 0.14" (40-lb tensile strength) cable ties to secure the Ethernet and sync cables to the cable guides on the module housing.

Figure 18: HSG-01 Housing

For the Ethernet cable tie, the Ethernet cable groove is molded lower at the top edge. For the sync cable tie, removal of a breakaway plug provides clearance for the sync cable, and removal of two breakaway side plates provides clearance for the sync cable tie.

5.2 FREQUENCY BAND RANGES

In the 2.4-, 5.2-, 5.4-, and 5.7-GHz frequency band ranges, Canopy APs, SMs, and BHs are available. Additionally, in the 900-MHz frequency band range, Canopy APs and SMs are available. To avoid self-interference, a Canopy network typically uses two or more of these ranges. For example, where properly arranged, all AP clusters and their respective SMs can use the 2.4-GHz range where the BH links use the 5.7-GHz range. In this scenario, subscriber links can span as far as 5 miles (8 km) with no reflector dishes, and the BH links can span as far as 35 miles (56 km) with reflector dishes on both ends.

Within this example network, wherever the 2.4-GHz is susceptible to interference from other sources, AP clusters and their linked SMs may use the 5.2-GHz range to span as far as 2 miles (3.2 km) with no reflector dishes. The network in this example takes advantage of frequency band range-specific characteristics of Canopy modules as follows:

- The 900-MHz modules cover a larger area, albeit with lower throughput, than modules of the other frequency bands. The 900-MHz modules can be used to
  - penetrate foliage
  - establish links that span greater distances
  - add subscribers
  - add overall throughput where modules of other frequency bands cannot be used (such as where interference would result or space on a tower is limited).

- The 2.4-GHz frequency band range supports AP/SM links of greater than 2-mile spans (with no reflectors).
- The 5.7-GHz frequency band range supports BH links that span as far as 35 miles.

5.3 CANOPY PRODUCT COMPARISONS

5.3.1 Canopy Product Applications

The product applications per frequency band range are is summarized in Table 10.

Table 10: Product applications per frequency band range

Product	Frequency Band Range				
	900 MHz	2.4 GHz	5.2 GHz	5.4 GHz	5.7 GHz
Access Point Module	●	●	●	●	●
Subscriber Module	●	●	●	●	●
Subscriber Module with Reflector[1]		●	●	●	●
Backhaul Module		●	●	●	●
Backhaul Module with Reflector[1]		●	●	●	●
Backhaul Module in 45-Mbps modulation					●
CMM2	●	●	●	●	●
CMMmicro	●	●	●	●	●
T1/E1 Multiplexer		●	●	●	●
Power supply	●	●	●	●	●
Surge suppressor	●	●	●	●	●

NOTES:

1. National or regional regulations apply. See National and Regional Regulatory Notices on Page 400.

5.3.2 Link Performance and Encryption Comparisons

The expected maximum range and throughput for Canopy links, with the type(s) of available encryption, is summarized in Table 11 and Table 12.

Table 11: Range, throughput, and encryption per frequency band range, PTMP links

Characteristic	Frequency Band Range				
	900 MHz	2.4 GHz	5.2 GHz	5.4 GHz	5.7 GHz
Range with Reflector		15 mi (24 km)		2 mi (3.2 km)	10 mi (16 km)
Range with no Reflector	40 mi (64 km)	5 mi (8 km)	2 mi (3.2 km)	2 mi (3.2 km)	2 mi (3.2 km)
Useful (data) aggregate throughput	2.2 Mbps	6.8 Mbps	6.8 Mbps	6.8 Mbps	6.8 Mbps
Encryption available	FIPS 197 AES, DES, or none	FIPS 197 AES, DES, or none	FIPS 197 AES, DES, or none	DES or none	FIPS 197 AES, DES, or none

Table 12: Range, throughput, and encryption per frequency band range, PTP links

Characteristic at Modulation Rate (Mbps)		Frequency Band Range				
		2.4 GHz	5.2 GHz	5.2 GHz ER	5.4 GHz	5.7 GHz
Range with Reflectors both ends	10	35 mi (56 km)		10 mi (16 km)	10 mi (16 km)	35 mi (56 km)
	20	35 mi (56 km)		5 mi (8 km)	5 mi (8 km)	35 mi (56 km)
	45					
Range with no Reflector	10	5 mi (8 km)	2 mi (3.2 km)		2 mi (3.2 km)	2 mi (3.2 km)
	20	3 mi (5 km)			1 mi (1.6 km)	1 mi (1.6 km)
	45					40 mi (64 km)[1]
Useful (data) aggregate throughput	10	7.5 Mbps	7.5 Mbps	7.5 Mbps	7.5 Mbps	7.5 Mbps
	20	14 Mbps		14 Mbps	14 Mbps	14 Mbps
	45					33.6 Mbps[2]
Encryption available	10	FIPS 197 AES, DES, or none	FIPS 197 AES, DES, or none	FIPS 197 AES, DES, or none	DES or none	FIPS 197 AES, DES, or none
	20	DES or none	DES or none	DES or none	DES or none	DES or none
	45					AES or none

NOTES:

1. The link calculator tool in the 45-Mbps BH should be used.
2. Data rates are dynamically variable from 3 to 33.6 Mbps aggregate throughput.

5.3.3 Cluster Management Product Comparison

Canopy offers a choice between two products for cluster management: CMM2 and CMMmicro. Your choice should be based on the installation environment and your requirements. The similarities and differences between these two products are summarized in Table 13.

Table 13: Cluster management product similarities and differences

Characteristic	CMM2	CMMmicro
Approximate size	17” H x 13” W x 6.5” D (43 cm H x 33 cm W x 7 cm D)	12” H x 10” W x 3” D (30 cm H x 25 cm W x 8 cm D)
Approximate weight	25 lb (11.3 kg)	8 lb (3.5 kg)
Cabling	◦ one Ethernet/power cable per radio. ◦ one sync cable per radio.	one Ethernet/power/sync cable per radio.
Canopy network interconnection	8 Ethernet ports	8 Ethernet ports
Data throughput	auto-negotiates to full or half duplex	auto-negotiates to full or half duplex
Ethernet operating speed standard	auto-negotiates to 10Base-T or 100Base-TX	auto-negotiates to 10Base-T or 100Base-TX
Additional Ethernet ports	one for data feed one for local access (notebook computer)	none
Power supply	integrated 24-V DC to power APs, BHs, and GPS receiver	external 24-V DC to power APs, BHs, and GPS receiver
SNMP management capability	none	provided
Sync (to prevent self-interference)	carried by the additional serial cable to each AP and BHM	embedded in power-over-Ethernet cable
Time & Date	carried by the additional serial cable to each AP and BHM	provided by NTP (Network Time Protocol). CMMmicro can be NTP server.
Weatherized	enclosure and power supply	only the enclosure (not the power supply)
Web interface	none	web pages for status, configuration, GPS status, and other purposes

5.4 ANTENNAS FOR CONNECTION TO 900-MHz MODULES

Like the 2.4-, 5.2-, 5.4-, and 5.7-GHz module, the 900-MHz module has

- the same housing.
- a covered Ethernet port.
- a utility port for alignment headset, sync cable to CMM2, or override plug.

The 900-MHz AP or SM is available with an integrated antenna or as a connectorized unit with a 16-inch (approximately 40-cm) cable with a male N-type connector for connection to the antenna.

5.4.1 Certified Connectorized Flat Panel Antenna from Motorola

Motorola has certified through regulatory agencies four connectorized flat panel antenna options. Motorola offers one of these, whose attributes include

- gain—10 dBi
- dimensions—8.8 x 8.1 x 1.6 inches (22.4 x 20.6 x 4.06 cm)
- weight—1.2 lbs (0.54 kg)
- polarization—vertical or horizontal
- cable—12-inch (30.5 cm)
- connector—female N-type
- beamwidth—approximately 60° vertical and 60° horizontal at 3 dBm

This antenna is pictured in Figure 3 on Page 38.

5.4.2 Other Certified Connectorized Flat Panel Antenna

Motorola has certified three other antennas, which are available through Canopy resellers. The attributes of one of these other certified antennas include

- gain—10 dBi
- dimensions—12 x12 x 1 inches (30.5 x 30.5 x 2.5 cm)
- weight—3.3 lbs (1.5 kg)
- polarization—vertical or horizontal
- connector—female N-type
- beamwidth—approximately 60° vertical and 60° horizontal at 3 dBm

This antenna is pictured in Figure 4 on Page 38.

5.4.3 Third-party Certified Connectorized Flat Panel Antenna

A third party may certify additional antennas for use with the Canopy connectorized 900-MHz module.

5.5 BANDWIDTH AND AUTHENTICATION MANAGER SOFTWARE

Canopy Bandwidth and Authentication Manager (BAM) software allows you to use

- a primary server to distribute bandwidth resources per subscriber, require SMs to authenticate per AP, and deny service to unauthorized SMs.
- a secondary server to redundantly store identical SM bandwidth and authentication data and become governing if the primary server goes out of service.
- an optional tertiary server to do the same if both the primary and secondary servers go out of service.

This product is supported by the dedicated document *Canopy Bandwidth and Authentication Manager User Guide* and associated release notes.

5.6 LICENSE MANAGER SOFTWARE

Under the previous licensing regime for Canopy networks, licenses were permanently tied to the Media Access Control (MAC) address of the equipment that was licensed or that used the licensed feature. Thus, they were not transferable. Under server-based license management, for some functionalities, Canopy offers licenses that

- float upon demand within the network.
- are tied to only the hostID (MAC address) of the license management server for which they were ordered.

In Release 4.2.3 and later releases, server-based license management adds flexibility and makes available licenses that previously would have been held by de-commissioned equipment. License management technology from Macrovision, based on a FLEXnet™ Publisher license management model, provides the platform for Canopy server-based licensing. Canopy capabilities that are authorized by licenses on this platform are *FLEXenabled* products.

In this platform, the license management server checks and then either assigns or declines to assign a license in real time. See the *Canopy Networks License Manager User Guide*.

5.7 SPECIFICATIONS AND LIMITATIONS

5.7.1 Radios

Canopy radio specifications are provided at http://motorola.canopywireless.com/prod_specs.php.

5.7.2 Cluster Management Products

Table 14: CMM2 specifications and limitations

Specification or Limitation	Canopy System Range
Max length from Cluster Management Module to any radio	328 cable feet (100 meters)
Max length from Cluster Management Module to GPS antenna	100 cable feet (30.5 meters)
Dimensions	17.00" H x 12.88" W x 6.50" D (43.18 cm H x 32.72 cm W x 16.51 cm D)
Weight	25.0 lbs. (11.3 kg)
Operation Temperature	-40°F to +131°F (-40°C to +55°C)
Overall	Meets CE IP44 according to EN60529:2000
AC Input Voltage and Frequency	100 V – 240 V~, 0.7 A – 0.35 A, settable to either 230 V or 115 V nominal input. 50 Hz – 60 Hz Note: Applying 230 V to a unit that is set to 115 V may damage the unit.
AC Input Power	Nominal 66 watts, max 92 watts with 8 modules connected to the CMM at max cable length.
24-V DC Input Voltage	18 to 32 V DC, measured at CMM
24-V DC Input Power	Nominal 60 watts. Maximum 84 watts with 8 modules connected to the CMM at maximum cable length. 9A inrush upon start-up.
24-V DC Usage	If using a typical "24V +/-5%" power supply, ensure that CMM is within 400 cable feet (120 m) of the power supply. Use minimum 12 AWG (4 mm^2) copper wire.
12-V DC Input Voltage	11.5 to 32 VDC, measured at CMM
12-V DC Usage	If using a 12V power source (typically an automobile battery in a test or emergency situation), use 12 AWG (4 mm^2) wire between the power supply and the CMM, ensure that the CMM is within 10 cable feet (3 m) of the power supply, and ensure the modules are within 20 cable feet (6 m) of the CMM.
Ethernet, GPS Sync, and GPS Coax Cables	The use of cables that conform to the operational temperature of the product as well as being UV light protected is mandatory.

Table 15: CMMmicro specifications and limitations

Specification or Limitation	Canopy System Range
Enclosure Size	Approximately 12” H x 10” W x 3” D (Approximately 30 cm H x 25 cm W x 7.5 cm D)
CMMmicro Weight (without DC power supply)	Approximately 8 lb (Approximately 3.5 k)
Max length from Cluster Management Module to any radio	328 cable feet (100 meters)
Max length from Cluster Management Module to GPS antenna	100 cable feet (30.5 meters)
Operating Temperature	-40°F to +131°F (-40°C to +55°C)
Provided DC Power Converter Input Voltage	100 – 240 V~
Provided DC Power Converter Input Frequency	50 – 60 Hz
CMMmicro Power Input Voltage	21.5 – 26.5 V DC
CMMmicro Power Current	3.36 A @ 24 V DC (3.75 – 3.0 A over voltage range)
Ethernet, GPS sync, and GPS coax cables	The use of cables that conform to the operational temperature of the product as well as having UV light protection is mandatory. Cables can be ordered from Best-Tronics Manufacturing, Inc. at http://www.best-tronics.com/motorola.htm.

5.7.3 300SS Surge Suppressor

Canopy Surge Suppressor specifications are provided at http://motorola.canopywireless.com/prod_specs.php.

6 DIFFERENTIATING AMONG COMPONENTS

For convenience, each Canopy module is labeled on the lower rear of the module cover, as shown in Figure 19.

Figure 19: Part and serial numbers, exterior label

The part number and serial number are reiterated above and between the cable jacks inside the module, as shown in Figure 20.

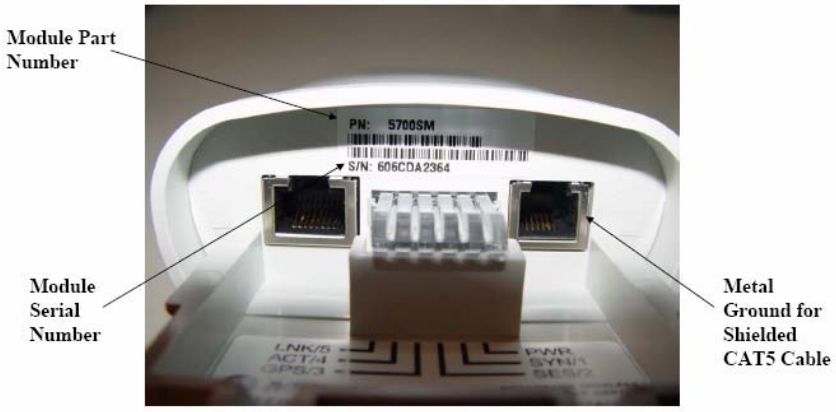


Figure 20: Part and serial numbers, interior label

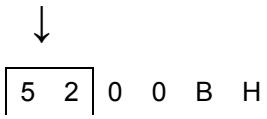
6.1 INTERPRETING PART NUMBER

The part number of a module sequentially indicates

- the model number, which indicates the
  - radio frequency band range.
  - link distance range.
  - the factory-set encryption standard.
- the module type.
- whether the reflector dish is included.
- the modulation capability.

Radio Frequency Band Range

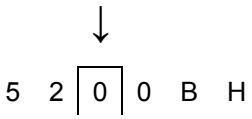
The leading digits indicate the frequency band range in which the module can operate. For example, if the part number is 5200BH, then the frequency band range of the module is 5.2 GHz.



You cannot change the frequency band range of the module.

Link Distance Range

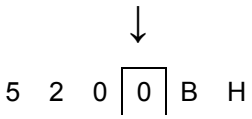
The next digit in the part number indicates whether the module is an extended range model. 1 indicates extended range. For example, if the part number is 5210BH, then the module *is* an extended range module. If the part number is 5200BH, then the module is not an extended range model.



You cannot change the link distance range of the module.

Encryption Standard

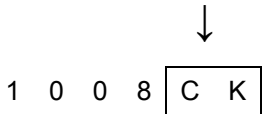
The next digit in the part number indicates the encryption standard that was preset at the factory. 1 indicates the Advanced Encryption Standard (AES). 0 indicates the Data Encryption Standard (DES) standard. For example, if the part number is 5201BH, then transmissions from the module are encrypted according to AES. If the part number is 5200BH, then transmissions from the module are encrypted according to DES.



You cannot change the encryption basis (from DES to AES, for example), but you can enable or disable the encryption.

Module Type

The next two alpha characters indicate the module type. For example, CK indicates that the module is a Cluster Management Module.

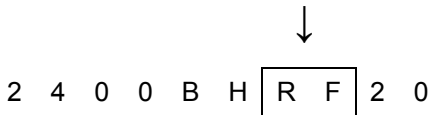


The module type cannot be changed.

Reflector Added

In specifications tables and price lists, the trailing characters RF or RF20 indicate that the associated information applies to the module being

- mounted to the 27RD Passive Reflector Dish, in the case of specifications.
- ordered with the 27RD Passive Reflector Dish, in the case of price lists.

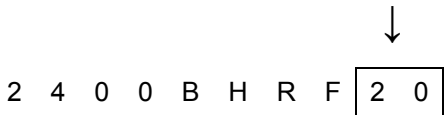


However, this designation is not shown on either label of the module, and a module ordered with the dish can be deployed without the dish.

Modulation Capability

A trailing 20 indicates that the module is capable of being set to either

- 20-Mbps modulation (aggregate throughput of 14 Mbps)
- 10-Mbps modulation (aggregate throughput of 7 Mbps).



The absence of a trailing 20 indicates that the module is capable of only 10-Mbps modulation.

6.2 INTERPRETING SERIAL NUMBER

The label shown in Figure 19 on Page 55 contains a serial number that is indicated by **S/N**. This is the Canopy product serial number. This number could be significant in your dealings with Motorola or your supply chain.

Figure 21: ESN and model numbers, other interior label

As shown in Figure 21, an **S/N** is also rendered on the interior label that identifies the status LED indicators. However, this is not the same **S/N** as above. This **S/N** is the electronic serial number (ESN), also know as the Media Access Control (MAC) address, of the module.

This hexadecimal number identifies the module in

- communications between modules.
- the data that modules store about each other.
- the data that the BAM software applies to manage authentication and bandwidth.

7 CANOPY LINK CHARACTERISTICS

7.1 UNDERSTANDING BANDWIDTH MANAGEMENT

7.1.1 Downlink Frame Contents

The AP broadcasts downlink frames that contain control information, allocating slots in succeeding or future uplink frames to SMs that have requested service. The downlink frame also contains a beacon frame, control information, and data that specific SMs have requested. Each SM

- examines the downlink frame to distinguish whether data is addressed to that SM.
- retrieves data addressed to that SM.
- directs such data to the appropriate user.

7.1.2 Uplink Frame Contents

Uplink frames contain control information from each SM that request service on succeeding uplink frames. SMs insert data into the uplink frames in an amount that the AP has established.

In a scenario in which 200 SMs (the maximum number of SMs that an AP can support) simultaneously request to pass data to the AP in the uplink frame, the AP acknowledges all of these requests within 80 msec. This interval is based on the frame size 2.5 msec, 400 frames per second, and 3 SMs per frame.

7.1.3 Frame Structure

With a 64-byte slot capacity, the Canopy frame consists of

- 33 data slots, subject to the following variables:
  - Maximum range decreases the number of available slots to 32.
  - Background bit error rate (BER) mode decreases the number of available data slots by one (and bandwidth by 200 kbps).
  - Every two control slots that are allocated decrease the number of available data slots by one.
- 6 control slots
  - 3 uplink control slots
  - 3 downlink control slots
- 6 acknowledgement slots
  - 3 uplink ACK slots
  - 3 downlink ACK slots

- 1 beacon slot, which identifies the
  - timing and distribution for the SMs
  - ratio of uplink to downlink allocation
  - ESN of the AP
  - color code
  - protocol (point-to-point or point-to-multipoint)
  - number of registered SMs
  - frame number
  - control slot information

When an SM boots, the following sequence occurs:

1. The SM finds this beacon slot from an AP.
2. The SM synchronizes with the AP.
3. If BAM is configured on the AP and the AP is licensed for authentication, then
   a. the AP sends a Registration Request message to the BAM server for authentication.
   b. following a successful challenge, the BAM server returns an Authentication Grant message to the AP.
   c. the AP sends a Registration Grant to the SM.

   If BAM *is not* configured on the AP or the AP is not licensed for authentication, then the AP simply returns the Registration Grant to the SM.

This Registration Grant includes the distance between the AP and SM. The SM uses the distance to distinguish when to transmit data in the uplink frame. The AP performs advance scheduling of up to 1024 frames that each SM will be permitted to use in the uplink frame.

ACK Slots

When the AP Status page is displayed and **Expanded Stats** has been selected, the Status page displays the total of ACK slots (1 through 7). In an ACK slot, the AP or SM sends to the other a bitmap, which tracks packet fragments.

Control Slots

When the AP Status page is displayed and **Expanded Stats** has been selected, the Status page displays the total of control slots (default 3, maximum 16). These control slots are contention slots. If too many SMs contend for these slots, then the number of control slots may be increased.

7.1.4 Media Access Control and AP Capacity

Regardless of whether the maximum number of SMs (200) all request service at the same time, the reservation Media Access Control (MAC) system allows the AP to give a reservation slot to each SM that requests service.

Regardless of the distance between any SM and the AP, the reservation MAC system ensures that all SM data slots are free of contention. For this reason

- all SMs are equally able to compete for uplink and downlink bandwidth.
- the capacity of the AP is not degraded by distance from the SMs.

7.1.5 Canopy Slot Usage

The frame illustrated in Figure 22 shows both packet fragments (yellow) and unused slot space (red) typical of uplink traffic. Packet sizes smaller than 64 bytes cause unused slot spaces.

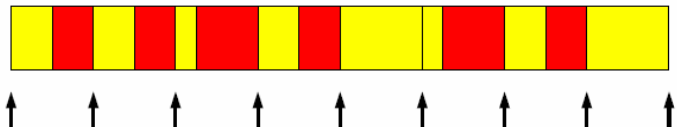


Figure 22: Uplink data slot usage

The following statistics apply to Canopy frame slot usage:

- Slot capacity is 64 bytes.
- The optimum Ethernet packet size is 1518 bytes.
- The maximum downlink throughput for one AP to one SM is 1800 pps.
- The maximum uplink throughput for one AP to one SM is 300 pps.
- The maximum backhaul throughput is 3000 pps.

7.1.6 Data Transfer Capacity

Canopy modules use Time Division Duplex (TDD) on a common frequency to divide frames for uplink (orange) and downlink (green) usage, as shown in Figure 23.

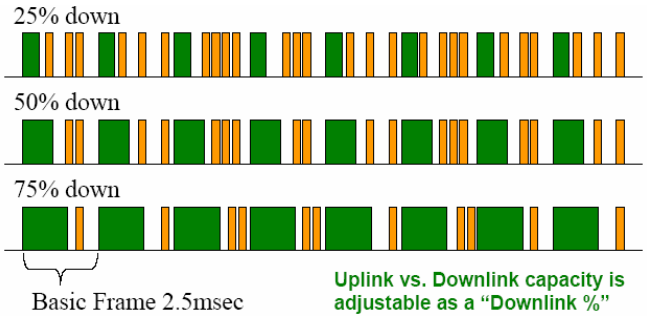


Figure 23: TDD dividing Canopy frames

7.1.7 QoS Parameters

Canopy point-to-multipoint links use the following four QoS parameters for bandwidth management:

- **Sustained Uplink Data Rate** (kbps)
- **Uplink Burst Allocation** (kb)
- **Sustained Downlink Data Rate** (kbps)
- **Downlink Burst Allocation** (kb)

You can independently set each of these parameters per AP or per SM.

Token Bucket Concept

The Canopy software uses a theoretical *token bucket* that

- stores credits (tokens) for the SM to spend on bandwidth for reception or transmission.
- drains tokens during reception or transmission.
- refills with tokens at the sustained rate set by the network operator.

For each token, the SM can send toward the network (or receive from the network) an equivalent number of kilobits. Each SM employs two buckets for the permitted throughput: one in the SM for uplink and one in the AP for downlink.

The **Uplink Burst Allocation** and **Downlink Burst Allocation** parameters in the AP or the BAM database establish the *number* of tokens that can fill each bucket. When the SM transmits (or receives) a packet, the equivalent number of tokens is removed from the uplink (or downlink) bucket.

- Except when full, the bucket is continuously being refilled with tokens at *rates* that the **Sustained Uplink Data Rate** and **Sustained Downlink Data Rate** parameters establish in the AP or the BAM database. The bucket often drains at a rate that is much faster than the sustained data rate but can refill at only the sustained data rate.

7.1.8 Maximum Information Rate (MIR)

A cap value specifies whether and how the aggregate (uplink plus downlink) throughput should be capped at a Maximum Information Rate (MIR). The uplink and downlink data rate caps are calculated as shown in Figure 24.

NOTE:
In these figures, *entry* refers to the setting in the data rate parameter, not the burst allocation parameter.

$$\text{uplink cap enforced} = \frac{\text{uplink entry} \times \text{aggregate cap for the SM}}{\text{uplink entry} + \text{downlink entry}}$$

$$\text{downlink cap enforced} = \frac{\text{downlink entry} \times \text{aggregate cap for the SM}}{\text{uplink entry} + \text{downlink entry}}$$

Figure 24: Uplink and downlink rate caps adjusted to apply aggregate cap

For example, in the Canopy SM, if you set the **Sustained Uplink Data Rate** parameter to 2,000 kbps and the **Sustained Downlink Data Rate** parameter to 10,000 kbps, then the uplink and downlink caps that will be enforced for the SM can be calculated as shown in Figure 25.

$$\text{uplink cap enforced} = \frac{2{,}000 \text{ kbps} \times 7{,}000 \text{ kbps}}{2{,}000 \text{ kbps} + 10{,}000 \text{ kbps}} = 1{,}167 \text{ kbps}$$

$$\text{downlink cap enforced} = \frac{10{,}000 \text{ kbps} \times 7{,}000 \text{ kbps}}{2{,}000 \text{ kbps} + 10{,}000 \text{ kbps}} = 5{,}833 \text{ kbps}$$

Figure 25: Uplink and downlink rate cap adjustment example

In this example case, the derived 1,167-kbps uplink and 5,833-kbps downlink caps sum to the fixed 7,000-kbps aggregate cap of the Canopy SM.

The sustained data rate and burst allocation parameters can be set either

- in the AP to apply to all SMs in the sector.
- in the SM (in Canopy System Release 6.1 and later).

7.1.9 Committed Information Rate

The Committed Information Rate (CIR) capability feature enables the service provider to guarantee to any subscriber that bandwidth will never decrease to below a specified minimum, unless CIR is oversubscribed. Bandwidth can be, and typically will be, higher than the minimum, but this guarantee helps the WISP to attract and retain subscribers.

In BAM Release 2.1 and later releases, BAM supports CIR capability as follows:

- Both the BAM GUI and the SSE command line interface allow you to view and change CIR configuration parameters per SM.
- When an SM successfully registers and authenticates, if BAM has CIR configuration data for the SM, then messages push the CIR configuration to the SM.
- BAM allows the CIR feature to be disabled in the SM without deleting the CIR configuration data.

7.1.10 Bandwidth from the SM Perspective

In the Canopy SM, normal web browsing, e-mail, small file transfers, and short streaming video are rarely rate limited with practical bandwidth management (QoS) settings in the AP or BAM. When the SM processes large downloads such as software upgrades and long streaming video or a series of medium-size downloads, the bucket rapidly drains, the burst limit is reached, and some packets are delayed. The subscriber experience is more affected in cases where the traffic is more latency sensitive.

7.1.11 Interaction of Burst Allocation and Sustained Data Rate Settings

If the Burst Allocation is set to 1200 kb and the Sustained Data Rate is set to 128 kbps, a data burst of 1000 kb is transmitted at full speed because the Burst Allocation is set high enough. After the burst, the bucket experiences a significant refill at the Sustained Data Rate. This configuration uses the advantage of the settable Burst Allocation.

If both the Burst Allocation and the Sustained Data Rate are set to 128 kb, a burst is limited to the Burst Allocation value. This configuration does not take advantage of the settable Burst Allocation.

If the Burst Allocation is set to 128 kb and the Sustained Data Rate is set to 256 kbps, the actual rate will be the burst allocation (but in kbps). As above, this configuration does not take advantage of the settable Burst Allocation.

A Burst Allocation value of zero prohibits all data transmission.

7.1.12 High-priority Bandwidth

To support low-latency traffic such as VoIP (Voice over IP) or video, the Canopy system implements a high-priority channel. This channel does not affect the inherent latencies in the Canopy system but allows high-priority traffic to be immediately served. The high-priority pipe separates low-latency from traffic that is latency tolerant, such as standard web traffic and file downloads.

The Canopy system separates this traffic by recognizing the IPv4 Type of Service (ToS) Low Latency bit (Bit 3). Bit 3 is set by a device outside the Canopy system. In the uplink frame, the SM monitors Bit 3. If this bit is set, then

- the SM prioritizes this traffic in its high-priority queue according to AP configuration settings for the high-priority channel.
- the system sends the packet on the high-priority channel and services this channel before any normal traffic.

NOTE:
To enable the high-priority channel, you must configure *all* high-priority parameters.

The high-priority channel is enabled by configuration of four parameters in the Configuration web page of the AP. These parameters are

- **High Priority Uplink Percentage**
- **UAcks Reserved High**
- **DAcks Reserved High**
- **NumCtrlSlots Reserved High**

IMPORTANT!
See High Priority Uplink Percentage and Slot Specifications on Page 191.

7.1.13 Allocations to Downlink and Uplink

The standard and high-priority channels in Canopy PTMP communications are contrasted in Figure 26 and Figure 27.

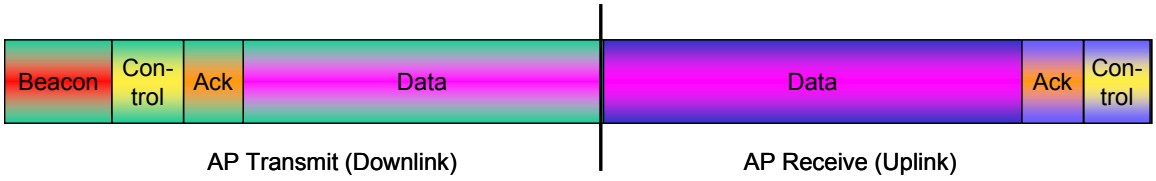


Figure 26: Canopy channel, 75% downlink, 0% high priority in uplink

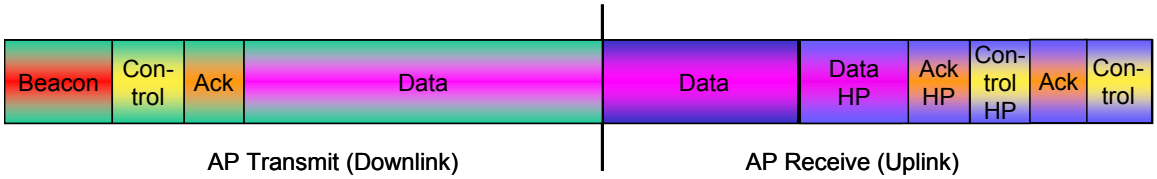


Figure 27: Canopy channel, 75 % downlink, 40 % high priority (HP) uplink, software scheduling

7.1.14 Software and Hardware Scheduling

In Release 6.0 and later, Canopy provides an alternative to software scheduling for control of the links in a sector. Hardware scheduling increases throughput and reduces latency in the link between the SM and AP.

With software scheduling and AP default downlink-to-uplink settings (75% downlink and 25% uplink), if High Priority is set to 25%, then

- in the uplink, the total of reserved slots is equivalent to 25% (2 slots in this example) and
  - the bandwidth is 64 bytes per slot, repeated 400 times each second.
  - [2 slots/instance] x [64 bytes/slot] x [8 bits/byte] x [400 instances/second] = 409,600 bps ≈ 400 kbps of uplink bandwidth
- in the downlink, the AP
  - monitors the Low Latency TOS (Type of Service) bit, Bit 3, in the Ethernet frame.
  - does not reserve slots, but will service all high-priority bandwidth requests.
  - can become saturated by attempting to service too much high-priority traffic.

Hardware scheduling always sends high-priority traffic first, even to the exclusion of other traffic.

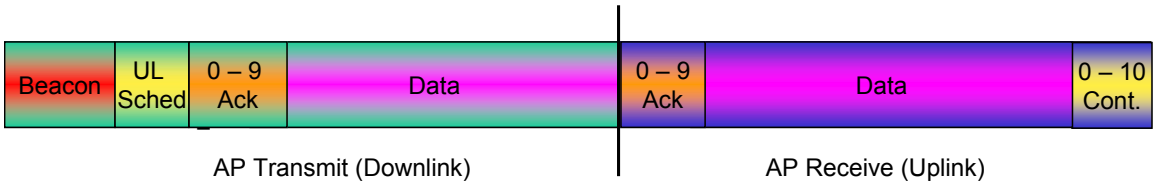


Figure 28: Canopy channel, 75%downlink, 40% high priority (HP) in uplink, hardware scheduling

IMPORTANT!
With Hardware Scheduling, the number of channels available to the AP is reduced by the number of SMs configured for the High Priority channel. With this feature enabled on all SMs, an AP can support only 100 SMs (instead of 200).

IMPORTANT!
In a Canopy BH link with Canopy T1/E1 Multiplexers, the BHs must be configured for an uplink/downlink ratio of 50% uplink/50% downlink. The Canopy T1/E1 Multiplexers are full duplex.

The differences between hardware and software scheduling in a Canopy sector are summarized in Table 16.

Table 16: Differences between software and hardware scheduling

Category	Factor	Difference	
		Software Scheduling	Hardware Scheduling
Throughput	Aggregate throughput, less additional overhead	6.8 Mbps	14 Mbps
	ACK slots in downlink used for data except when request for uplink is present	No	Yes
Latency	Number of frames required for the scheduling process	5	1
	Round-trip latency[1]	≈ 20 ms	≈ 6 ms
	AP broadcast the download schedule	Yes	No
High-priority Channel	Allocation for *uplink* high-priority traffic on amount of high-priority traffic	Static, based on fixed percentage	Dynamic, based on amount of high-priority traffic
	Allocation for *downlink* high-priority traffic on amount of high-priority traffic	Dynamic, based on amount of high-priority traffic	Dynamic, based on amount of high-priority traffic
	Order of transmission	1. Any high-priority 2. Any low-priority	1. CIR high-priority 2. CIR low-priority 3. Other high-priority 4. Other low-priority
Transmit Frame Spreading	Support for Transmit Frame Spreading feature	In all releases	In Release 7.0 and later
CIR	Capability	None	In all releases
NOTES: 1. For 2.4- and 5.*n*-GHz modules.			

7.1.15 Settable AP Broadcast Repeat Count

In Release 4.2 and later releases, a settable parameter controls how many times, in addition to the original broadcast, the AP repeats each broadcast. You can set this parameter to achieve high reliability or high throughput, or a compromise between these, based on the type and amount of traffic that the AP broadcasts. For a description of conditions where each allowed setting can be best, see Broadcast Repeat Count on 191.

7.2 UNDERSTANDING SYNCHRONIZATION

Although Canopy modules are band selective, they are not channel selective. For this reason, the receiver of a module can receive too much signal from unsynchronized modules that are operating in the same spectrum (frequency band range, such as 5.2 GHz). This would overload the front end of the receiver, which would cancel the carrier-to-interference (C/I) ratio advantage of Canopy modules.

Moreover, Canopy modules must be synchronized so that they transmit and receive in the proper cycles. An unsynchronized module that transmits during the receive cycle of another module can render the other module insensitive to the desired signal (desensed).

7.2.1 GPS Synchronization

The Navigation Satellite Timing and Ranging (NAVSTAR) Global Positioning System (GPS) uses 24 satellites to relay information for precise derivation of position and time.

The Canopy Cluster Management Module (CMM) contains a Motorola Oncore GPS Receiver. The CMM is a critical element in the operation of the Canopy system. At one AP cluster site or throughout an entire wireless system, the CMM provides a GPS timing pulse to each module, synchronizing the network transmission cycles.

The Oncore GPS Receiver tracks eight or more satellites. The CMM uses the signal from at least four of these satellites to generate a one-second interval clock that has a rise time of 100 nsec. This clock directly synchronizes APs and BHMs which, in turn, synchronize all other modules in the Canopy network.

The Oncore GPS Receiver also provides

- the latitude and longitude of the GPS antenna (collocated with the CMM)
- the number of satellites that are being tracked
- the number of satellites that are available
- the date
- the time in Universal Coordinated Time (UCT)
- the altitude of the GPS antenna
- other information that can be used to diagnose network problems.

Alternative to GPS Sync

A Canopy link can operate without GPS sync, but cannot operate without sync. The alternative to GPS sync is to configure the AP or BHM in the link to generate a sync pulse to pass to the SM or BHS, respectively. Depending on the RF environment in which the link operates, this latter alternative may or may not be plausible.

For example, in Figure 29, AP4

- is not synchronized with any of the other APs.
- is transmitting nearby the other APs while they are expecting to receive SM transmissions from a maximum distance.

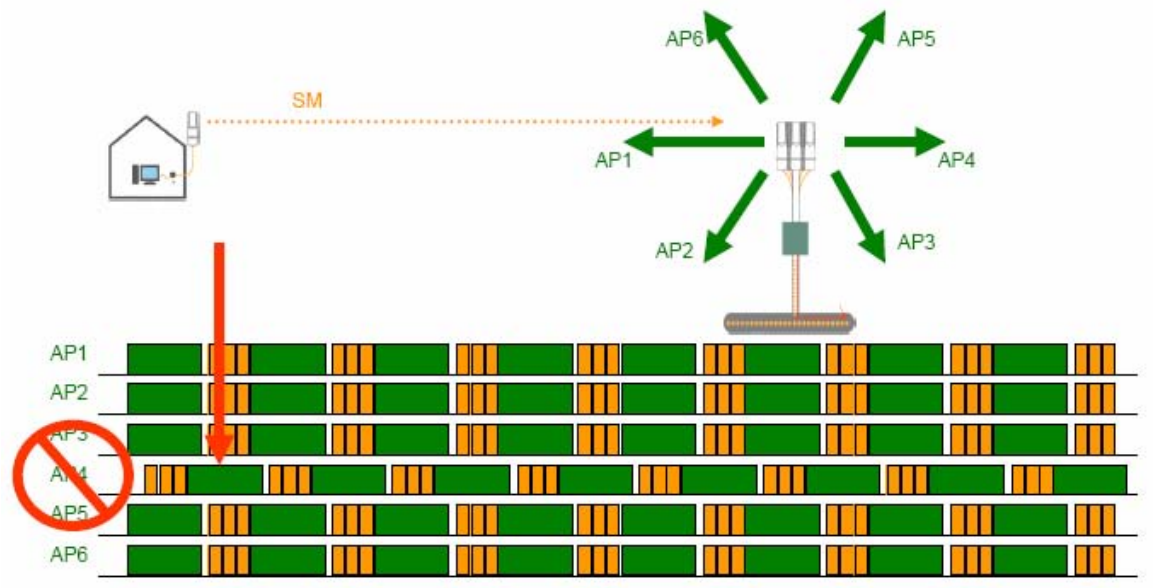


Figure 29: One unsynchronized AP in cluster

The result is self-interference. In this scenario, the self-interference can be avoided only by synchronizing the TDD transmit cycles of all APs that operate in the same frequency band.

An AP that is isolated by at least 5 miles (8 km) from any other Canopy equipment, or a BHM in an isolated standalone BH link can generate and pass sync pulse without GPS timing and not risk that interference will result from the generated sync. In any other type of Canopy link, sync should be derived from GPS timing.

NOTE:
The 45-Mbps BHM generates its own sync. For more information about this module, see the *Canopy 45-Mbps Backhaul User Guide*.

Advantage of GPS Sync

Although the embedded timing generation capability of the Canopy AP and BHM keeps a precise clock, no trigger exists to start the clock at the same moment in each AP of a cluster. So, the individual AP can synchronize communications between itself and registered SMs, but cannot synchronize itself with other Canopy modules, except by GPS timing (shown in Figure 30).

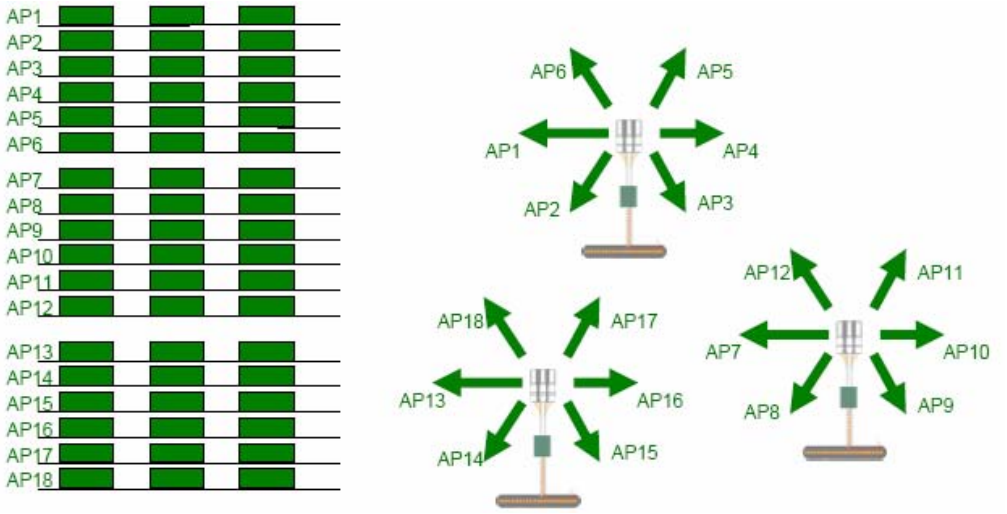


Figure 30: GPS timing throughout the Canopy network

7.2.2 Passing Sync in a Single Hop

In releases earlier than Release 4.0, network sync can be delivered in only one over the air link in any of the following network designs:

- Design 1
  1. A CMM provides sync to a collocated AP.
  2. This AP sends the sync over the air to SMs.
- Design 2
  1. A CMM provides sync to a collocated BH timing master.
  2. This BH timing master sends the sync over the air to a BH timing slave.

7.2.3 Passing Sync in an Additional Hop

In Release 4.0 and later releases, network sync can be either delivered as described above or extended by one additional link in any of the following network designs:

NOTE:
In each of these following designs, Link 2 *is not* on the same frequency band as Link 4. (For example, Link 2 may be a 5.2-GHz link while Link 4 is a 5.7- or 2.4-GHz link.)

- Design 3
  1. A CMM provides sync to a collocated AP.
  2. This AP sends the sync over the air to an SM.
  3. This SM delivers the sync to a collocated AP.
  4. This AP passes the sync in the additional link over the air to SMs.

This design is illustrated in Figure 31.

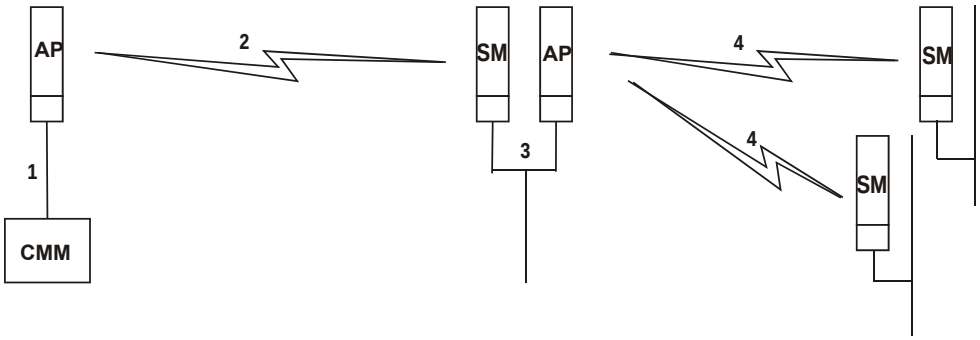


Figure 31: Additional link to extend network sync, Design 3

- Design 4
  1. A CMM provides sync to a collocated AP.
  2. This AP sends the sync over the air to an SM.
  3. This SM delivers the sync to a collocated BHM.
  4. This BHM passes the sync in the additional link over the air to a BHS.

This design is illustrated in Figure 32.

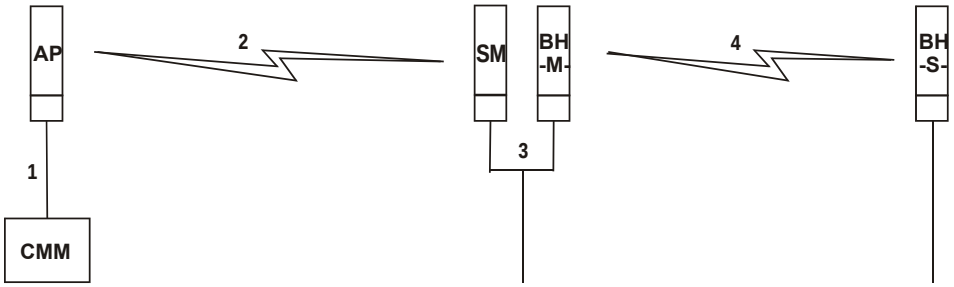


Figure 32: Additional link to extend network sync, Design 4

- Design 5
  1. A CMM provides sync to a collocated BHM or the BHM generates timing.
  2. This BHM sends the sync over the air to a BHS.
  3. This BHS delivers the sync to a collocated AP.
  4. This AP passes the sync in the additional link over the air to SMs.

This design is illustrated in Figure 33.

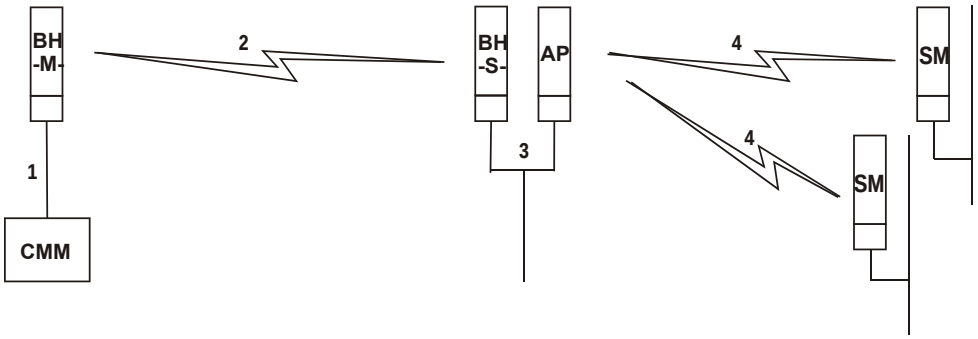


Figure 33: Additional link to extend network sync, Design 5

Wiring and configuration information for this sync extension is described under Wiring to Extend Network Sync on Page 294.

8 MEETING LINK REQUIREMENTS

8.1 AP-SM LINKS

8.1.1 AP-SM Link Distances

APs and Subscriber Modules are available in 900-MHz, 2.4-GHz, 5.2-GHz, 5.4-GHz, and 5.7-GHz frequency bands. Due to regulatory agency restrictions, a 5.2-GHz SM *cannot* be used with a reflector in the U.S.A. or Canada. A 2.4-GHz or 5.7-GHz SM can be used with a Canopy Passive Reflector dish. This reflector extends the maximum span of a link.

For a 900-MHz AP-SM link, the range in typical conditions is 40 miles (64 km). However, you can set the 900-MHz AP to a range as great as 120 miles (more than 190 km) to establish links across longer distances where the Fresnel zone is clear and the RF environment is uncontested.

For a 2.4-GHz AP-SM link, the maximum distance is

- 15 mi (24 km) with the reflector on the SM.
- 5 mi (8 km) with no reflector.

NOTE:
Greater distances with the reflector may be attempted for 2.4-GHz links. See Max Range on Page 195.

For a 5.2-GHz AP-SM link, the maximum distance is 2 mi (3.2 km) with no dish.

For a 5.4-GHz AP-SM link, the maximum distance is 2 mi (3.2 km) with or without a reflector.

For a 5.7-GHz AP-SM link, the maximum distance is

- 10 mi (16 km) with the reflector on the SM.
- 2 mi (3.2 km) with no reflector.

8.1.2 AP-SM Data Transfer

Point-to-multipoint Capacity

Canopy APs communicate with SMs using a point-to-multipoint protocol. An AP-SM link has lower throughput and higher latency than a backhaul link for two reasons:

- Many endpoints are involved.
- The bandwidth request and reservation process consumes bandwidth.

In the 900-MHz frequency band range, round-trip latency is typically

- 40 msec with software scheduling.
- 15 msec with hardware scheduling.

In all other Canopy frequency band ranges, round-trip latency is typically

- 20 msec with software scheduling.
- 6 msec with hardware scheduling.

At range settings of greater than 40 miles (64 km) in the 900-MHz AP, more time elapses between transmit and receive cycles to compensate for greater air delay. In each frame, this reduces the number of data slots, which slightly reduces the aggregate throughput of the link. However, the throughput is as predictable as in other Canopy point-to-multipoint links.

Throughput is a factor of the **Max Range** parameter in the AP and is effective for all SMs, regardless of their distance from the AP. The aggregate useful throughput for each AP in the other Canopy frequency band ranges is 6.2 Mbps with software scheduling (7 Mbps with hardware scheduling), regardless of the downlink percentage setting. This throughput includes all downlink data to all SMs and all uplink data from all SMs that link to the AP.

The downlink throughput to a single SM can be greater than 4 Mbps. The uplink throughput to an AP can be as great as approximately 2 Mbps, depending on the uplink/downlink ratio. However, setting the ratio to 50% for a point-to-mulitpoint Canopy link does not yield an even division of bandwidth between uplink and downlink traffic. This is evident in the throughput values that are quoted in Table 17 and Table 18.

NOTE:
These values were derived from the Link Test web pages of Canopy modules. For the link tests, the **Total NumUAckSlots**, **NumDAckSlots**, and **NumCtlSlots** parameters were set to the default value of 3.

Table 17: Downlink and uplink PTMP throughput, 2-mile link, software scheduling

Downlink Percent	Data Slots Down	Data Slots Up	Downlink Throughput (MHz)	Uplink Throughput (MHz)
95	31	2	4.9	0.4
90	30	3	5.1	0.5
85	28	5	5.6	0.8
80	26	7	4.9	1.1
75	25	8	4.9	1.2
70	23	9	4.4	1.3
65	21	11	3.9	1.5
60	20	12	3.9	1.6
55	18	14	3.6	1.7
50	16	16	3.3	1.9
45	15	17	3.0	2.0

Downlink Percent	Data Slots Down	Data Slots Up	Downlink Throughput (MHz)	Uplink Throughput (MHz)
40	13	19	2.6	2.1
35	11	21	2.2	2.3
30	10	22	2.0	2.2
25	8	23	1.6	2.4
20	6	25	1.2	2.4
15	5	26	1.0	2.6
10	3	28	0.6	2.5
5	2	29	0.4	2.7
0	1	29	0.4	2.7

Table 18: Downlink and uplink PTMP throughput, 15-mile link, software scheduling

Downlink Percent	Data Slots Down	Data Slots Up
95	29	2
90	28	3
85	26	4
80	25	5
75	23	7
70	21	9
65	20	10
60	18	12
55	17	13
50	15	15
45	14	16
40	12	18
35	10	19
30	9	20
25	7	22
20	6	23
15	4	25
10	3	26

Downlink Percent	Data Slots Down	Data Slots Up
5	2	27
0	2	27

Changing Network Conditions

The effects of changing network conditions on PTMP throughput are indicated in Table 19.

Table 19: Effects of network conditions on PTMP throughput

Changing Network Condition	Effect on Throughput		
	Aggregate AP	Short Link	Long Link
Increasing the **Max Range** parameter setting in the AP	somewhat decreased[1]	somewhat decreased, but equals that of a long link	somewhat decreased, but equals that of a short link
Increasing the number of SMs that register in the AP	no effect		
Increase in downlink traffic			
Increase in uplink traffic			
Increasing the average bandwidth allotted to the SMs that register in the AP	no effect, even when the additional bandwidth is used.	depends on subscriber usage of the additional bandwidth, but equals that of a long link	depends on subscriber usage of the additional bandwidth, but equals that of a short link

NOTES:

1. To avoid a decrease of unnecessary proportion, set as not much further than the distance between the AP and the furthest SM that registers in the AP.

8.2 BH-BH LINKS

8.2.1 BH-BH Link Distances

Backhaul modules are available in

- 2.4-, 5.2-, and 5.4-GHz frequency bands in 10- and 20-Mbps data transfer rates
- 5.7-GHz frequency band in 10- and 20- and 45-Mbps data transfer rates

NOTE:
The 45-Mbps BH is supported by the dedicated document *Canopy 45-Mbps Backhaul User Guide*.

Select BHs based on desired data handling capability, desired link range, and whether the BHs will either operate in a network environment or be collocated with an AP or AP cluster.

2.4-, 5.4-, and 5.7-GHz BHs can be used with a reflector on either or both ends. In the U.S.A. and Canada, regular 5.2-GHz backhauls *cannot* be used with a reflector, due to regulatory agency restrictions. However, Extended Range (ER) 5.2-GHz BHs use very low transmit power and are permitted with a reflector in the U.S.A. and Canada, as well as elsewhere. Where these Extended Range BHs are deployed, reflectors on both ends are recommended.

On either or both ends of a link, a Canopy Passive Reflector dish extends the transmission and reception range of the BH.

For a 2.4-GHz BH link, the maximum distance is

- 35 mi (56 km) with the dish on both ends.
- 15 mi (24 km) with the dish on one end at 10-Mbps modulation.
- 5 mi (8 km) with the dish on one end at 20-Mbps modulation.
- 5 mi (8 km) with no dish at 10-Mbps modulation.
- 3 mi (4.8 km) with no dish at 20-Mbps modulation.

For a 5.2-GHz BH link, the maximum distance is

- 10 mi (16 km) with the dish on both ends in 10-Mbps modulation, except that the dish is not allowed on Model 5200 in the U.S.A. or Canada.
- 5 mi (8 km) with the dish on both ends in 20-Mbps modulation.
- 2 mi (3.2 km) with the dish on
  - one end in 10-Mbps modulation.
  - neither end in Model 5200.
- 1 mi (1.6 km) with the dish on one end in 20-Mbps modulation.

For a 5.4- or 5.7-GHz BH link, the maximum distance is

- 35 mi (56 km) with the dish on both ends.
- 10 mi (16 km) with the dish on one end in 10-Mbps modulation.
- 5 mi (8 km) with the dish on one end in 20-Mbps modulation.
- 2 mi (3.2 km) with no dish at 10-Mbps modulation.
- 1 mi (1.6 km) with no dish at 20-Mbps modulation.

8.2.2 BH-BH Data Transfer

Point-to-point Capacity

Canopy BHs communicate with each other using a point-to-point protocol. This point-to-point protocol uses a 2.5-msec frame. A BH link has higher throughput and lower latency (typically 5 msec, 2.5 msec in each direction) for two reasons:

- Only two endpoints are involved.
- No bandwidth request and reservation process is involved.

For 10-Mbps BHs, the aggregate throughput on the channel is 7 Mbps. For 20-Mbps BHs, the aggregate throughput on the channel is 14 Mbps. If a BH is set to a downlink ratio of 50%, then the bandwidth in each direction is half of the total BH link bandwidth.

9 PREVIEWING NETWORK CONFIGURATIONS

The following are examples of network layouts. Customer experience case studies are also available.

9.1 VIEWING TYPICAL LAYOUTS

The following layouts are typical of Canopy system implementations:

- Figure 34: Typical network layout with no BH
- Figure 35: Typical network layout with BH
- Figure 36: Typical multiple-BH network layout

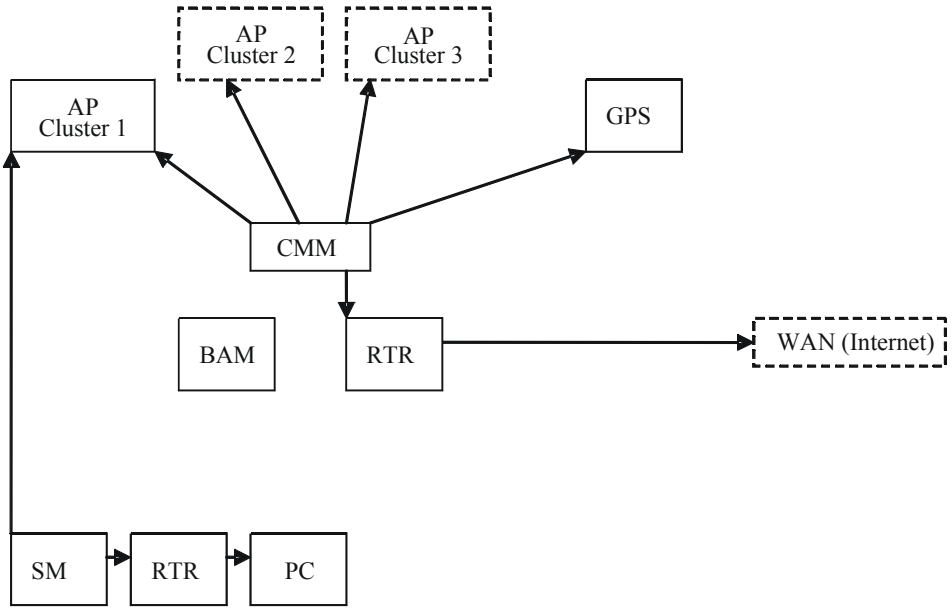


Figure 34: Typical network layout with no BH

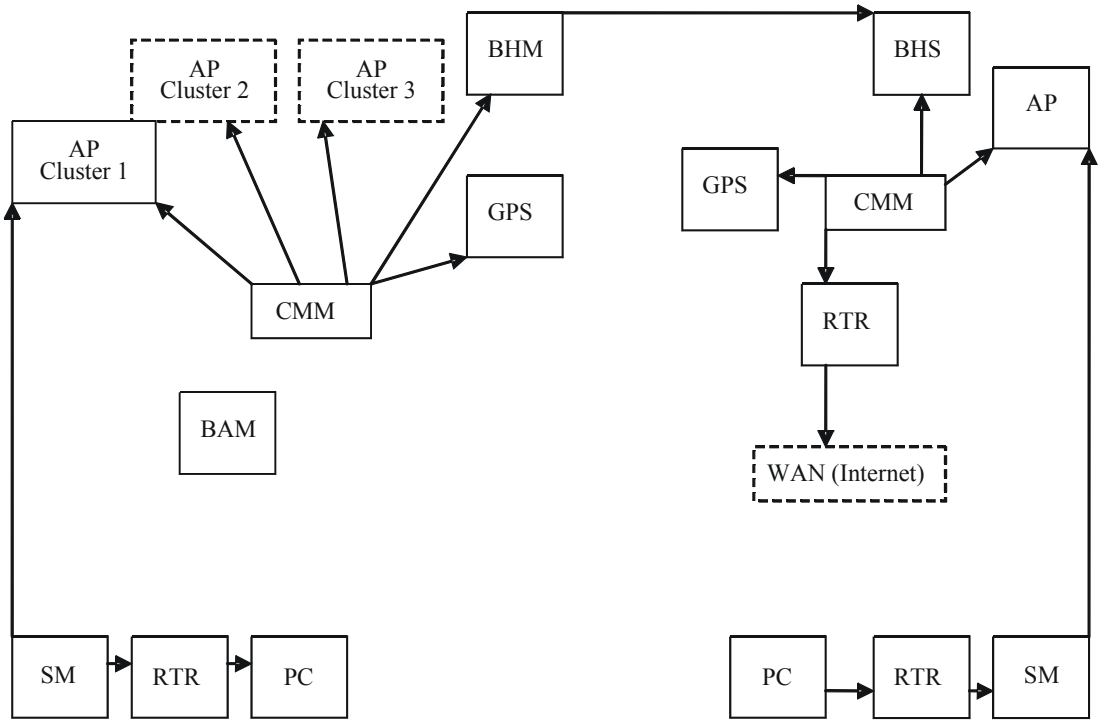


Figure 35: Typical network layout with BH

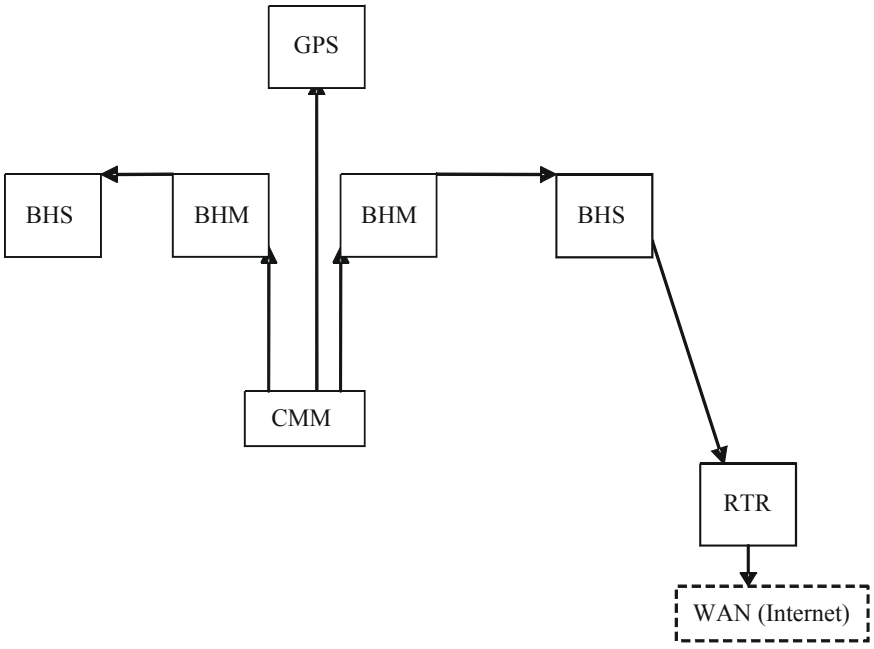


Figure 36: Typical multiple-BH network layout

9.2 VIEWING CASE STUDIES

Case studies of Canopy implementations are available as “Feature Articles” for download from http://www.connectwithcanopy.com/index.cfm?canopy=menu.case.

10 ACCESSING FEATURES

In successive software releases, Canopy includes new features that improve aspects such as cost, efficiency, flexibility, installation, interference avoidance, security, throughput, and troubleshooting. Improvements that Canopy features offer are indicated in Table 20.

Table 20: Canopy features and their benefits

Feature Name	Initial Software Release	Category of Improvement								
		Cost	Efficiency	Fix	Flexibility	Installation	Interference	Security	Throughput	Troubleshooting
Software Limit Increase on **2.4-GHz Module** (from 15 to 30 Miles)	4.2.1	●			●					
2.4-GHz Module P9 Support	4.2.7				●					
5.2-GHz Module P9 Support	4.2.7				●					
5.4-GHz Module P9 Support	4.2.7				●					
5.7-GHz Module Support	3.1.5				●					
5.7-GHz Module ISM Frequencies Support	4.0				●		●			
5.7-GHz Module P9 Support	4.2.3				●					
900-MHz Module (all P9) Support	4.2.2				●					
Release 6.0 Compatibility Mode for **900-MHz Module**	6.1				●					
Advanced Encryption Standard (**AES**) Encryption	4.0							●		
Enhanced **Alignment** Mode	3.1.5					●				
Audible **Alignment Tone**	4.0					●				
Audible **Alignment Tone** on Only SMs and BHSs Fix	4.0.2			●						
New **Alignment Tone** for P9 Boards	4.2.3					●				
Alignment Tone Fix	6.1			●						
Network **Archive** Maintenance	CNUT 1.0		●							
BH 64-byte Packet **Asynchronicity** Fix	4.2.1			●						
BH **Authentication**	4.0							●		
Floating Licenses for APs with **Authentication**	4.2.3	●	●			●				
Shorter than 32 Hex **Authentication** Keys Accepted	4.2.3		●		●					

Feature Name	Initial Software Release	Category of Improvement								
		Cost	Efficiency	Fix	Flexibility	Installation	Interference	Security	Throughput	Troubleshooting
Auto Detection of SMs, Versions, and States	CNUT 1.0		●							
SM **Auto Update**	4.1		●							
Batch **Auto Updates**	CNUT 1.0		●							
Bus Bandwidth Limitation Causing 20-Mbps **BH Errors** Fix	4.0.1			●						
CANOPY**BOOT** Version 3.0 Fix (Replaces Version 2.5)	4.2.3			●						
BHM **Bridge** Changes	3.1.5							●		
Bridge Table from 256 to 4096 Entries	3.1.5				●					
Configurable **Bridge Table** Timeout	3.1.5				●					
Settable AP **Broadcast Repeat** Count	4.2.1								●	
Committed Information Rate (**CIR**) with Hardware Scheduler	6.1				●					
Configuration Source Parameter at AP for VLAN, MIR, and CIR	6.1		●							
Data Encryption Standard (**DES**) Encryption	3.1.5							●		
Dynamic Frequency Selection (**DFS**) for 5.7-GHz Module	4.2.3			●						
5.4-GHz Module Dynamic Frequency Selection (**DFS**) for Radar	4.2.7			●						
DHCP Server and Client in SM	4.1		●							
DHCP Client Sends Lease Renewals as Unicast Fix	4.2.3								●	
Demilitarized Zone (**DMZ**) in SM	4.1				●			●		
Wrongly Reported **DMZ** IP Conflict with DHCP Server IP Range Fix	4.2.1			●						
DMZ Host as FTP Client Fix	4.2.3			●						
Default **Downlink** Percentages: AP 75%, BH 50%	3.1.5								●	
Encrypted **Downlink** Broadcast	4.2.1							●		
Disable SM **Ethernet Interface**	3.2		●					●		●
Protocol and Port **Filtering**	4.2.1							●		
Improved Protocol and Port **Filtering**	4.2.3							●		

Feature Name	Initial Software Release	Category of Improvement								
		Cost	Efficiency	Fix	Flexibility	Installation	Interference	Security	Throughput	Troubleshooting
Consistent Display of **FPGA** as 6 digits	4.2.3			●						
Oversized (Up to 1532 Bytes) Ethernet **Frame** Fix	3.2			●						
Frame Calculator for Tuning Mixed Clusters	6.1						●			
Transmit **Frame Spreading**	4.0						●			
All **Frames** Adjusted for Cross-release Communications	6.1				●					
GPS Antenna Connection Status	4.0									●
Telnet Corrupting **GPS** Information Fix	4.0.4			●						
BH **Hash Table** Fix	3.2			●						
900-MHz Module Dynamic per-SM **High-priority Channel** with Hardware Scheduler	6.0				●					
Dynamic per-SM **High-priority Channel** with Hardware Scheduler	6.1				●					
Public **IP Access** for SM	3.1.5				●					
Public **IP Access** for BHS	3.1.5				●					
ISM State Preserved through Reset to Factory Defaults Fix	4.0.2			●						
Improved **Jitter** Control	4.0						●			
20-Mbps BH **Jitter** Measurement Fix	4.0.1			●						
900-MHz Module Hardware Scheduler Reduced **Latency**	6.0				●					
Reduced **Latency** with Hardware Scheduler	6.1				●					
Server-based **License** Management	License Mgr 1.0	●	●			●				
Customer **Logo** on Web-based Interface	3.1.5				●					
Configurable Hyperlinked **Logo**	4.2.1		●							
BH Configurable for **Master or Slave**	3.1.5				●					
Canopy Enterprise **MIB**	3.2		●							●
Updated Canopy Enterprise **MIB**	4.0		●							●
Updated Canopy Enterprise **MIB**	4.1		●							●
Updated Canopy Enterprise **MIB**	4.2.1		●							●

Feature Name	Initial Software Release	Category of Improvement								
		Cost	Efficiency	Fix	Flexibility	Installation	Interference	Security	Throughput	Troubleshooting
Updated Canopy Enterprise **MIB**	4.2.3		●							●
Maximum Information Rate (**MIR**) Settable at SM	6.1 and BAM 2.1				●					
20-Mbps BH to 10-Mbps BH **Modulation**	4.0					●				
MySQL Database Support	BAM 1.0				●					
Network Address Translation (**NAT**) in SM	4.1				●			●		
NAT Support for VPNs—L2TP Over IPSec	4.2.1							●		
Passwords on FTP and Telnet Sessions	3.1.5							●		
PostgreSQL Database Support	BAM 2.0		●		●					
Low **Power** Mode (18-dB Reduction)	4.1				●		●			
5.4-GHz Module Adjustable **Power**	4.2.7				●		●			
2.4-GHz Module Adjustable **Power**	4.2.7				●		●			
5.7-GHz Module Adjustable **Power** with Connectorized Antenna	6.1				●		●			
Power Level Measurement	4.0					●				●
RADIUS Database Support	BAM 2.0				●					
Display **Registered AP**	4.0					●				●
Registration Failed SM List	4.0									●
No **Remote Access**	4.0							●		
Default **Router** Change for BHS	3.1.5				●					
Default **Router** Change for SM	3.1.5				●					
Improved Received Signal Strength Indicator (**RSSI**)	4.0					●				
SM **Scan** Privacy	4.0							●		
SM and BHS **Site Names** in AP or BHM Sessions Page	4.2.1		●							
SNMP Manager and SM Subnet Address Fix	4.2.1			●						
Spectrum Analyzer in SM and BHS	4.1		●			●	●			
Graphical **Spectrum Analyzer** in SM and BHS	4.2.1		●							
PDA Info and **Spectrum Analyzer** Pages	4.2.1		●			●	●			

Feature Name	Initial Software Release	Category of Improvement								
		Cost	Efficiency	Fix	Flexibility	Installation	Interference	Security	Throughput	Troubleshooting
900-MHz Module **Spectrum Analyzer** in AP	6.0					●	●			
Spectrum Analyzer in AP	6.1					●	●			
Suspend or reinstate SM through the BAM GUI	BAM 2.0		●							
GPS **Sync** Protection	3.1.5						●			
Extended Network with **Sync**	4.0	●			●		●			
Telnet Commands Defined	4.2.1		●		●					
900-MHz Module Hardware Scheduler Increased **Throughput**	6.0								●	
Increased **Throughput** with Hardware Scheduler	6.1								●	
Time & Date for APs or BHMs Connected to CMMmicro	4.2.1 and CMMmicro 2.1									●
VLAN (802.1Q)	6.1				●			●		
Web Pages Remain Scrolled	4.2.1		●							

10.1 ACTIVATING FEATURES

A Canopy feature is active if the software that allows the feature to be turned on or off (enabled or disabled) is present.

10.1.1 Fixed License Keys

Some features are activated by loading a fixed license key into the radio. Such a key arrives from Motorola as a *filename*.url file. When you double-click on this file, your browser opens and the location bar is populated by a lengthy string. This URL string begins with http://<*ModuleIPAddress*>/. If you need to load a key into a module whose IP address has changed since Motorola issued the key, perform the following steps.

Procedure 1: Modifying a fixed license key for a module IP address

1. Right-click on the license key filename.
2. Select **Properties**.
3. Select the **Web Document** tab.
4. At **URL**, substitute the current IP address for the original IP address in the URL.
5. Click **OK**.

6. Double-click on the license key filename.
   RESULT: The key loads into the module.
7. Open the Configuration web page of the module.
8. Review parameter settings and enable the feature if you wish to do so at this time (see next section).

end of procedure

10.2 ENABLING FEATURES

A Canopy feature is enabled (functioning) if the feature is both active and enabled. For example, Transmit Frame Spreading is active (can be enabled) in any AP or BHM that operates on Release 4.0 or a later release. However, Transmit Frame Spreading functions only if the **Enable** selection for the **Transmit Frame Spreading** parameter is checked in the Configuration web page of the module.

11 ACQUIRING PROFICIENCIES

Designing and operating a Canopy network requires fundamental knowledge of radio frequency transmission and reception, Internet Protocol addressing schemes, experimentation with Canopy equipment, and for most operators participation in some forms of Canopy training.

11.1 UNDERSTANDING RF FUNDAMENTALS

Canopy training and user interfaces presume an understanding of RF fundamentals. Excellent written sources for these fundamentals are available. One such source is *Deploying License-Free Wireless Wide-Area Networks* by Jack Unger (ISBN 1-58705-069-2), published by Cisco Press.

11.2 UNDERSTANDING IP FUNDAMENTALS

Canopy training and user interfaces also presume an understanding of Internet Protocol (IP) fundamentals. Excellent written sources for these fundamentals are similarly available. One such source is *Sams Teach Yourself TCP/IP in 24 Hours* by Joe Casad (ISBN 0-672-32085-1), published by Sams Publishing.

NOTE:
The default IP address of each Canopy component is 169.254.1.1.

11.3 ACQUIRING A CANOPY DEMONSTRATION KIT

Canopy Demonstration Kits are available through your Canopy representative.

11.3.1 900-MHz Demonstration Kit

Each 900-MHz Demonstration Kit contains:

- 2 SMs
- 1 AP
- 3 AN900 Connectorized (External) Antennas
- 1 300SS Surge Suppressor
- 1 SMMB1 SM Mounting Bracket
- 3 ACPS110-03 110-V AC Power Supplies[2]
- 3 CBL-0562 Straight-through Category 5 Cables
- 1 CBL-0565 Crossover Category 5 Cable
- 1 UGTK-0001 Trial Kit Quick Start Guide
- 1 CPT001-CD02EN Sales Overview on CD

[2] Included in only Demonstration Kit TK1004.

- 1 CPT002-CD02EN Technical Overview on CD
- 1 CPT003-CD03EN Canopy System User Guide on CD

Part numbers for Demonstration Kits are provided in Table 21.

11.3.2 2.4-GHz Demonstration Kit

Each 2.4-GHz Demonstration Kit contains:

- 2 SMs
- 1 AP
- 1 300SS Surge Suppressor
- 1 SMMB1 SM Mounting Bracket
- 1 27RD Reflector Dish Kit
- 3 ACPS110-03 110-V AC Power Supplies[3]
- 3 ACPSSW-02 90- to 230-V AC Power Supplies[4]
- 3 CBL-0562 Straight-through Category 5 Cables
- 1 CBL-0565 Crossover Category 5 Cable
- 1 UGTK-0001 Trial Kit Quick Start Guide
- 1 CPT001-CD02EN Sales Overview on CD
- 1 CPT002-CD02EN Technical Overview on CD
- 1 CPT003-CD03EN Canopy System User Guide on CD

Part numbers for Demonstration Kits are provided in Table 21.

11.3.3 5.2-GHz Demonstration Kit

Each 5.2-GHz Demonstration Kit contains:

- 2 SMs
- 1 AP
- 1 300SS Surge Suppressor
- 1 SMMB1 SM Mounting Bracket
- 3 ACPS110-03 110-V AC Power Supplies[5]
- 3 ACPSSW-02 90- to 230-V AC Power Supplies[6]
- 3 CBL-0562 Straight-through Category 5 Cables
- 1 CBL-0565 Crossover Category 5 Cable
- 1 UGTK-0001 Trial Kit Quick Start Guide
- 1 CPT001-CD02EN Sales Overview on CD
- 1 CPT002-CD02EN Technical Overview on CD

---

[3] Included in only Demonstration Kit TK10007.

[4] Included in only Demonstration Kit TK10008.

[5] Included in only Demonstration Kit TK10003.

[6] Included in only Demonstration Kit TK10005.

- 1 CPT003-CD03EN Canopy System User Guide on CD

Part numbers for Demonstration Kits are provided in Table 21.

11.3.4 5.4-GHz Demonstration Kit

Each 5.4-GHz Demonstration Kit contains:

- 2 SMs
- 1 AP
- 1 300SS Surge Suppressor
- 1 SMMB1 SM Mounting Bracket
- 3 ACPSSW-02 90- to 230-V AC Power Supplies
- 3 CBL-0562 Straight-through Category 5 Cables
- 1 CBL-0565 Crossover Category 5 Cable
- 1 UGTK-0002 Trial Kit Quick Start Guide
- 1 CPT001-CD02EN Sales Overview on CD
- 1 CPT002-CD02EN Technical Overview on CD
- 1 CPT003-CD03EN Canopy System User Guide on CD

11.3.5 5.7-GHz Demonstration Kit

Each 5.7-GHz Demonstration Kit contains:

- 2 SMs
- 1 AP
- 1 300SS Surge Suppressor
- 1 SMMB1 SM Mounting Bracket
- 1 27RD Reflector Dish Kit
- 3 ACPS110-03 110-V AC Power Supplies[7]
- 3 ACPSSW-02 90- to 230-V AC Power Supplies
- 3 CBL-0562 Straight-through Category 5 Cables
- 1 CBL-0565 Crossover Category 5 Cable
- 1 UGTK-0001 Trial Kit Quick Start Guide
- 1 CPT001-CD02EN Sales Overview on CD
- 1 CPT002-CD02EN Technical Overview on CD
- 1 CPT003-CD03EN Canopy System User Guide on CD

Part numbers for Demonstration Kits are provided in Table 21.

[7] Included in only Demonstration Kit TK10004.

Table 21: Demonstration Kit part numbers

Frequency Band Range	Power Supply Input (Volts AC)	Part Number
900 MHz	110	TK10010
2.4 GHz	110	TK10007
	230	TK10008
5.2 GHz	110	TK10003
	230	TK10005
5.4 GHz	230	TK10013
5.7 GHz	110	TK10004
	230	TK10006

11.4 ACQUIRING A CANOPY STARTER KIT

Canopy Starter Kits are also available through your Canopy representative.

11.4.1 900-MHz Starter Kit

Each 900-MHz Starter Kit contains:

- 20 SMs
- 3 APs
- 23 AN900 Connectorized (External) Antennas
- 1 1070CK CMMmicro
- 21 300SS Surge Suppressors
- 20 SMMB1 SM Mounting Brackets
- 20 ACPS110-03 110-V AC Power Supplies
- 1 UGTK-0002 Quick Start Guide
- 1 CPT003-CD02EN Canopy System User Guide on CD

Part numbers for Starter Kits are provided in Table 22.

11.4.2 2.4-GHz Starter Kit

Each 2.4-GHz Starter Kit contains:

- 30 SMs
- 6 APs
- 1 1008CK-2 CMM2
- 31 300SS Surge Suppressors
- 15 SMMB1 SM Mounting Brackets
- 15 27RD Reflector Dish Kits

- 30 ACPS110-03 110-V AC Power Supplies[8]
- 30 ACPSSW-02 90- to 230-V AC Power Supplies[9]
- 1 CTCAT5-01 Category 5 Cable Tester[10]
- 1 UGTK-0002 Quick Start Guide
- 1 CPT003-CD02EN Canopy System User Guide on CD

Part numbers for Starter Kits are provided in Table 22

11.4.3 5.2-GHz Starter Kit

Each 5.2-GHz Starter Kit contains:

- 30 SMs
- 6 APs
- 1 1008CK-2 CMM2
- 31 300SS Surge Suppressors
- 30 SMMB1 SM Mounting Brackets
- 30 ACPS110-03 110-V AC Power Supplies[11]
- 30 ACPSSW-02 90- to 230-V AC Power Supplies[12]
- 1 CTCAT5-01 Category 5 Cable Tester[13]
- 1 UGTK-0002 Quick Start Guide
- 1 CPT003-CD02EN Canopy System User Guide on CD

Part numbers for Starter Kits are provided in Table 22.

11.4.4 5.4-GHz Starter Kit

Each 5.4-GHz Starter Kit contains:

- 30 SMs
- 6 APs
- 1 1008CK-2 CMM2
- 31 300SS Surge Suppressors
- 30 SMMB1 SM Mounting Brackets
- 30 ACPSSW-02 90- to 230-V AC Power Supplies
- 1 UGSK-0003 Quick Start Guide
- 1 CPT003-CD02EN Canopy System User Guide on CD

---

[8] Included in only Starter Kit TK10035.

[9] Included in only Starter Kit TK10036.

[10] Included in only TK10035.

[11] Included in only Starter Kit TK10031.

[12] Included in only Starter Kit TK10033.

[13] Included in only TK10031.

Part numbers for Starter Kits are provided in Table 22.

11.4.5 5.7-GHz Starter Kit

Each 5.7-GHz Starter Kit contains:

- 30 SMs
- 6 APs
- 1 1008CK-2 CMM2
- 31 300SS Surge Suppressors
- 15 SMMB1 SM Mounting Brackets
- 15 27RD Reflector Dish Kits
- 30 ACPS110-03 110-V AC Power Supplies[14]
- 30 ACPSSW-02 90- to 230-V AC Power Supplies[15]
- 1 CTCAT5-01 Category 5 Cable Tester[16]
- 1 UGTK-0002 Quick Start Guide
- 1 CPT003-CD02EN Canopy System User Guide on CD

Part numbers for Starter Kits are provided in Table 22.

Table 22: Starter Kit Part Numbers

Frequency Band Range	Power Supply Input (Volts AC)	Part Number
900 MHz	110	TK10028
2.4 GHz	110	TK10035
	230	TK10036
5.2 GHz	110	TK10031
	230	TK10033
5.4 GHz	230	TK10039
5.7 GHz	110	TK10032
	230	TK10034

11.5 EVALUATING CANOPY TRAINING OPTIONS

Canopy and its distributors make technical training available to customers. For information on this training, either

- send email inquiries to training@canopywireless.com.
- visit http://www.motorola.com/canopy, click on **Services**, the click on **Training**.

[14] Included in only Starter Kit TK10032.

[15] Included in only Starter Kit TK10034.

[16] Included in only TK10032.

11.6 ATTENDING ON-LINE KNOWLEDGE SESSIONS

Irregularly but often, Canopy presents a knowledge session over the Internet about a new product offering. Some of these knowledge sessions provide the opportunity for participants to interact in real time with the leader of the session.

The knowledge session

- provides a high-level understanding of the technology that the new product introduces.
- announces any subtleties and caveats.
- typically includes a demonstration of the product.
- is usually recorded for later viewing by those who could not attend in real time.

To participate in upcoming knowledge sessions, ask your Canopy representative to ensure that you receive email notifications.

DESIGNING YOUR CANOPY NETWORK

12 ENGINEERING YOUR RF COMMUNICATIONS

Before diagramming network layouts, the wise course is to

- anticipate the correct amount of signal loss for your fade margin calculation.
- recognize all significant RF conditions.
- evaluate potential sites by their fitness to address fade margin and ambient RF conditions.

12.1 ANTICIPATING RF SIGNAL LOSS

The C/I (Carrier-to-Interference) ratio defines the strength of the intended signal relative to the collective strength of all other signals. Canopy modules typically have an especially low C/I ratio of

- 3 dB or less at 10-Mbps modulation.
- 10 dB or less at 20-Mbps modulation.

The C/I ratio is alternatively known as jitter. The C/I ratio is typically a design feature of the radio.

12.1.1 Understanding Attenuation

An RF signal in space is attenuated by atmospheric and other effects as a function of the distance from the initial transmission point. The further a reception point is placed from the transmission point, the weaker is the received RF signal.

12.1.2 Calculating Free Space Path Loss

The attenuation that distance imposes on a signal is the free space path loss. PathLossCalcPage.xls calculates free space path loss.

12.1.3 Calculating Rx Signal Level

The Rx sensitivity of each module is stated under Specifications and Limitations on Page 52. The determinants in Rx signal level are illustrated in Figure 37.

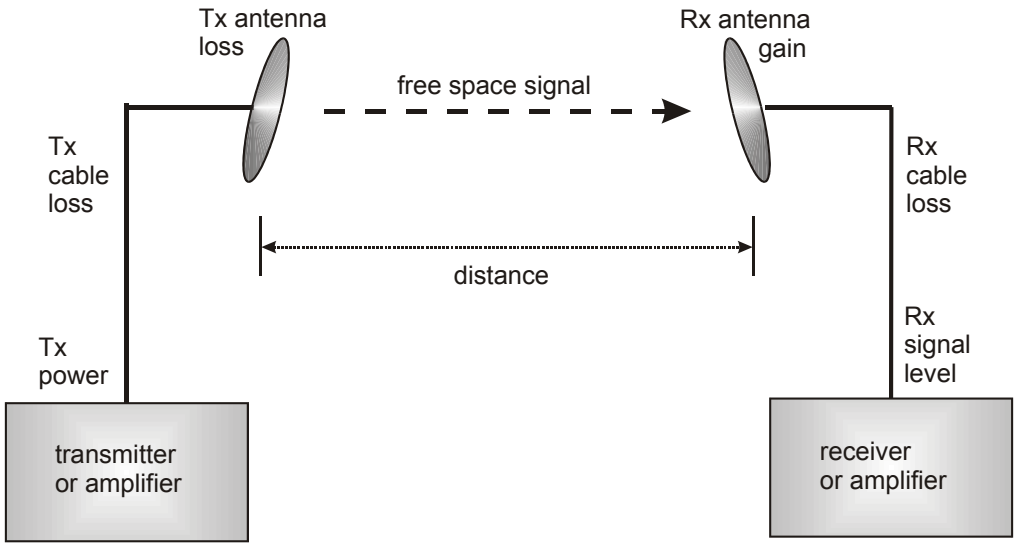


Figure 37: Determinants in Rx signal level

Rx signal level is calculated as follows:

Rx signal level dB = *Tx power* − *Tx cable loss* + *Tx antenna gain*
− *free space path loss* + *Rx antenna gain* − *Rx cable loss*

NOTE:
This Rx signal level calculation presumes that a clear line of sight is established between the transmitter and receiver and that no objects encroach in the Fresnel zone.

12.1.4 Calculating Fade Margin

Free space path loss is a major determinant in Rx (received) signal level. Rx signal level, in turn, is a major factor in the system operating margin (fade margin), which is calculated as follows:

system operating margin (fade margin) **dB =*Rx signal level* dB − *Rx sensitivity* dB**

12.2 ANALYZING THE RF ENVIRONMENT

An essential element in RF network planning is the analysis of spectrum usage and the strength of the signals that occupy the spectrum you are planning to use. Regardless of how you measure and log or chart the results you find (through the Spectrum Analyzer in SM and BHS feature or by using a spectrum analyzer), you should do so

- at various times of day.
- on various days of the week.
- periodically into the future.

As new RF neighbors move in or consumer devices in your spectrum proliferate, this will keep you aware of the dynamic possibilities for interference with your network.

12.2.1 Mapping RF Neighbor Frequencies

In Release 4.1 and later releases, you can

- use an SM or BHS, or an AP in Release 6.1 or later, as a spectrum analyzer.
- view a table (or graphical display in Release 4.2 or a later release) that shows power level in RSSI and dBm for each frequency throughout the entire 20-MHz range, regardless of limited selections in the **Custom RF Frequency Scan Selection List** field of the SM Configuration page.
- select an AP channel that minimizes interference from other RF equipment.

You can use this functionality during the alignment of an SM, but you may find it especially helpful for frequency selection during site planning. The Spectrum Analyzer in SM and BHS feature provides this functionality.

The SM measures only the spectrum of its manufacture. So if, for example, you wish to analyze an area for both 2.4- and 5.7-GHz activity, take both a 2.4- and 5.7-GHz SM to the area. To enable this functionality, perform the following steps:

CAUTION!
The following procedure causes the SM to drop any active RF link. If a link is dropped when the spectrum analysis begins, the link can be re-established when either a 15-minute interval has elapsed or the spectrum analyzer feature is disabled.

Procedure 2: Analyzing the spectrum

1. Predetermine a power source and interface that will work for the SM or BHS in the area you want to analyze.
2. Take the SM or BHS, power source, and interface device to the area.
3. Access the Expanded Stats page of the SM or BHS.
4. On the Expanded Stats page, click **Spectrum Analyzer**.
5. On the Spectrum Analyzer page, click **Enable**.
   RESULT: The feature is enabled.

6. Click **Enable** again.
   RESULT: The system measures RSSI and dBm for each frequency in the spectrum.
7. Travel to another location in the area.
8. Click **Enable** again.
   RESULT: The system provides a new measurement of RSSI and dBm for each frequency in the spectrum.
   NOTE: Spectrum analysis mode times out 15 minutes after the mode was invoked in Step 5.
9. Repeat Steps 7 and 8 until the area has been adequately scanned and logged.

As with any other data that pertains to your business, a decision today to put the data into a retrievable database may grow in value to you over time.

RECOMMENDATION:
Wherever you find the measured noise level is greater than the sensitivity of the radio that you plan to deploy, use the noise level (rather than the link budget) for your link feasibility calculations.

12.2.2 Anticipating Reflection of Radio Waves

In the signal path, any object that is larger than the wavelength of the signal can reflect the signal. Such an object can even be the surface of the earth or of a river, bay, or lake. The wavelength of the signal is approximately

- 2 inches for 5.2- and 5.7-GHz signals.
- 5 inches for 2.4-GHz signals.
- 12 inches for 900-MHz signals.

A reflected signal can arrive at the antenna of the receiver later than the non-reflected signal arrives. These two or more signals cause the condition known as multipath. When multipath occurs, the reflected signal cancels part of the effect of the non-reflected signal so, overall, attenuation beyond that caused by link distance occurs. This is problematic at the margin of the link budget, where the standard operating margin (fade margin) may be compromised.

12.2.3 Noting Possible Obstructions in the Fresnel Zone

The Fresnel (pronounced *fre·NEL*) Zone is a theoretical three-dimensional area around the line of sight of an antenna transmission. Objects that penetrate this area can cause the received strength of the transmitted signal to fade. Out-of-phase reflections and absorption of the signal result in signal cancellation.

The foliage of trees and plants in the Fresnel Zone can cause signal loss. Seasonal density, moisture content of the foliage, and other factors such as wind may change the amount of loss. Plan to perform frequent and regular link tests if you must transmit though foliage.

12.2.4 Radar Signature Detection and Shutdown

In Release 4.2.3 and later releases, the Dynamic Frequency Selection (DFS) for United Kingdom feature in the 5.7-GHz AP and BHM senses military radar and shuts down the radio. The 5.4-GHz AP and BHM likewise sense military radar and shut down. The shutdown of an AP/BHM effectively shuts down the SMs/BHS, which transmit only while receiving the beacon of the AP/BHM.

When an AP or BHM in this frequency band range is enabled for DFS, the radio scans for a radar signature throughout the first minute after a boot. During this or any later scan, if the radio detects radar, then the radio

1. shuts down for the next 30 minutes.
2. re-scans for one minute.

However, the scan delay is unfavorable where regulations do not require radar signature detection and shutdown. For this reason

- the default state of the **DFS** parameter in the Configuration page of the AP/BHM is **Disabled**.
- the network operator where radar signature detection and shutdown is required must toggle the **DFS** parameter to **Enabled**
  - when the module is first deployed.
  - if ever the parameters have been reset to factory defaults.

RECOMMENDATION:
Where regulations require that radar sensing and radio shutdown is enabled, you can most effectively share the spectrum with satellite services if you perform spectrum analysis and select channels that are distributed evenly across the frequency band range.

12.3 CONSIDERING FREQUENCY BAND ALTERNATIVES

For 5.2-, 5.4-, and 5.7-GHz modules, 20-MHz wide channels are centered every 5 MHz. For 2.4-GHz modules, 20-MHz wide channels are centered every 2.5 MHz. This allows the operator to customize the channel layout for interoperability where other Canopy equipment is collocated.

Cross-band deployment of APs and BH is the recommended alternative (for example, a 5.2-GHz AP collocated with 5.7-GHz BH).

IMPORTANT!
Regardless of whether 2.4-, 5.2-, 5.4-, or 5.7-GHz modules are deployed, channel separation between modules should be at least 20 MHz.

Channel selections for the AP in the 2.4-GHz band depend on whether the AP is deployed in cluster.

12.3.1 900-MHz Channels

12.3.2 900-MHz Single AP Available Channels

A single 900-MHz AP can operate with the 8-MHz wide channel centered on any of the following frequencies:

(All Frequencies in MHz)

906	907	911	915
919	923	924	

900-MHz AP Cluster Recommended Channels

Three non-overlapping channels are recommended for use in a 900-MHz AP cluster:

(All Frequencies in MHz)

906	915	924

This recommendation allows 9 MHz of separation between channel centers. You can use the Spectrum Analysis feature in an SM, or use a standalone spectrum analyzer, to evaluate the RF environment. In any case, ensure that the 8-MHz wide channels you select *do not* overlap.

12.3.3 2.4-GHz Channels

2.4-GHz BH and Single AP Available Channels

A BH or a single 2.4-GHz AP can operate in the following channels, which are separated by only 2.5-MHz increments.

(All Frequencies in GHz)

2.4150	2.4275	2.4400	2.4525
2.4175	2.4300	2.4425	2.4550
2.4200	2.4325	2.4450	2.4575
2.4225	2.4350	2.4475	
2.4250	2.4375	2.4500	

The channels of *adjacent* 2.4-GHz APs should be separated by at least 20 MHz.

2.4-GHz AP Cluster Recommended Channels

Three non-overlapping channels are recommended for use in a 2.4-GHz AP cluster:

(All Frequencies in GHz)

2.4150	2.4350	2.4575

This recommendation allows 20 MHz of separation between one pair of channels and 22.5 MHz between the other pair. You can use the Spectrum Analysis feature in an SM or BHS, or use a standalone spectrum analyzer, to evaluate the RF environment. Where spectrum analysis identifies risk of interference for any of these channels, you can compromise this recommendation as follows:

- Select 2.4375 GHz for the middle channel
- Select 2.455 GHz for the top channel
- Select 2.4175 GHz for the bottom channel

In any case, ensure that your plan allows at least 20 MHz of separation between channels.

12.3.4 5.2-GHz Channels

Channel selections for the AP in the 5.2-GHz frequency band range depend on whether the AP is deployed in cluster.

5.2-GHz BH and Single AP Available Channels

A BH or a single 5.2-GHz AP can operate in the following channels, which are separated by 5-MHz increments.

(All Frequencies in GHz)

5.275	5.290	5.305	5.320
5.280	5.295	5.310	5.325
5.285	5.300	5.315	

The channels of *adjacent* APs should be separated by at least 20 MHz. However, 25 MHz of separation is advised.

5.2-GHz AP Cluster Recommended Channels

Three non-overlapping channels are recommended for use in a 5.2-GHz AP cluster:

(All Frequencies in GHz)

5.275	5.300	5.325

12.3.5 5.4-GHz Channels

Channel selections for the AP in the 5.4-GHz frequency band range depend on whether the AP is deployed in cluster.

5.4-GHz BH and Single AP Available

A BH or single 5.4-GHz AP can operate in the following channels, which are separated by 5-MHz.

(All Frequencies in GHz)

5495	5515	5535	5555	5575	5595	5615	5635	5655	5675	5695
5500	5520	5540	5560	5580	5600	5620	5640	5660	5680	5700
5505	5525	5545	5565	5585	5605	5625	5645	5665	5685	5705
5510	5530	5550	5570	5590	5610	5630	5650	5670	5690	

The channels of *adjacent* APs should be separated by at least 20 MHz.

5.4-GHz AP Cluster Recommended Channels

The fully populated cluster requires only three channels, each reused by the module that is mounted 180° opposed. In this frequency band range, the possible sets of three non-overlapping channels are numerous.

IMPORTANT!

Where regulations require you to have Dynamic Frequency Selection (DFS) enabled, analyze the spectrum, then spread your channel selections as evenly as possible throughout this frequency band range, appropriately sharing it with satellite services.

12.3.6 5.7-GHz Channels

Channel selections for the AP in the 5.7-GHz frequency band range depend on whether the AP is deployed in cluster.

5.7-GHz BH and Single AP Available ISM/U-NII Channels

A BH or a single 5.7-GHz AP enabled for ISM/U-NII frequencies can operate in the following channels, which are separated by 5-MHz increments.

(All Frequencies in GHz)

5.735	5.765	5.795	5.825
5.740	5.770	5.800	5.830
5.745	5.775	5.805	5.835
5.750	5.780	5.810	5.840
5.755	5.785	5.815	
5.760	5.790	5.820	

The channels of *adjacent* APs should be separated by at least 20 MHz. However, 25 MHz of separation is advised.

5.7-GHz AP Cluster Recommended ISM/U-NII Channels

Six non-overlapping ISM/U-NII channels are recommended for use in a 5.7-GHz AP cluster:

(All Frequencies in GHz)

5.735	5.775	5.815
5.755	5.795	5.835

The fully populated cluster requires only three channels, each reused by the module that is mounted 180° offset. The six channels above are also used for backhaul point-to-point links.

As noted above, a 5.7-GHz AP enabled for ISM/U-NII frequencies can operate on a frequency as high as 5.840 GHz. Where engineering plans allow, this frequency can be used to provide an additional 5-MHz separation between AP and BH channels.

12.3.7 5.8-GHz Channels Available for 45-Mbps Backhaul Module

Channel selections for the 45-Mbps BH are as follows:

(All Frequencies in GHz)

5.734	5.764	5.794	5.824
5.740	5.770	5.800	5.830
5.746	5.776	5.806	5.836
5.752	5.782	5.812	5.842
5.758	5.788	5.818	

12.3.8 Example Channel Plans for AP Clusters

Examples for assignment of frequency channels and sector IDs are provided in the following tables. Each frequency is reused on the sector that is at a 180° offset. The entry in the Symbol column of each table refers to the layout in Figure 38 on Page 106.

NOTE:
The operator specifies the sector ID for the module as described under Sector ID on Page 334.

Table 23: Example 900-MHz channel assignment by sector

Direction of Access Point Sector	Frequency	Sector ID	Symbol
North (0°)	906 MHz	0	A
Northeast (60°)	915 MHz	1	B
Southeast (120°)	924 MHz	2	C
South (180°)	906 MHz	3	A
Southwest (240°)	915 MHz	4	B
Northwest (300°)	924 MHz	5	C

Table 24: Example 2.4-GHz channel assignment by sector

Direction of Access Point Sector	Frequency	Sector ID	Symbol
North (0°)	2.4150 GHz	0	A
Northeast (60°)	2.4350 GHz	1	B
Southeast (120°)	2.4575 GHz	2	C
South (180°)	2.4150 GHz	3	A
Southwest (240°)	2.4350 GHz	4	B
Northwest (300°)	2.4575 GHz	5	C

Table 25: Example 5.2-GHz channel assignment by sector

Direction of Access Point Sector	Frequency	Sector ID	Symbol
North (0°)	5.275 GHz	0	A
Northeast (60°)	5.300 GHz	1	B
Southeast (120°)	5.325 GHz	2	C
South (180°)	5.275 GHz	3	A
Southwest (240°)	5.300 GHz	4	B
Northwest (300°)	5.325 GHz	5	C

Table 26: Example 5.4-GHz channel assignment by sector

Direction of Access Point Sector	Frequency	Sector ID	Symbol
North (0°)	5.580 GHz	0	A
Northeast (60°)	5.620 GHz	1	B
Southeast (120°)	5.660 GHz	2	C
South (180°)	5.580 GHz	3	A
Southwest (240°)	5.620 GHz	4	B
Northwest (300°)	5.660 GHz	5	C

Table 27: Example 5.7-GHz channel assignment by sector

Direction of Access Point Sector	Frequency	Sector ID	Symbol
North (0°)	5.735 GHz	0	A
Northeast (60°)	5.755 GHz	1	B
Southeast (120°)	5.775 GHz	2	C
South (180°)	5.735 GHz	3	A
Southwest (240°)	5.755 GHz	4	B
Northwest (300°)	5.775 GHz	5	C

12.3.9 Multiple Access Points Clusters

When deploying multiple AP clusters in a dense area, consider aligning the clusters as shown in Figure 38. However, this is only a recommendation. An installation may dictate a different pattern of channel assignments.

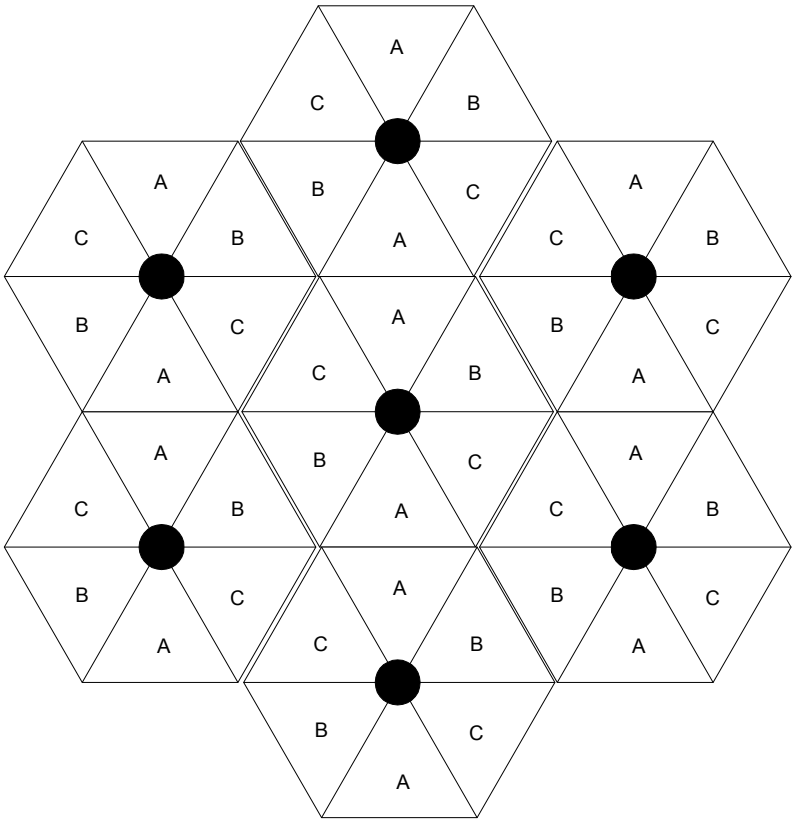


Figure 38: Example layout of 7 Access Point clusters

12.4 SELECTING SITES FOR NETWORK ELEMENTS

The Canopy APs must be positioned

- with hardware that the wind and ambient vibrations cannot flex or move.
- where a tower or rooftop is available or can be erected.
- where a grounding system is available.
- with lightning arrestors to transport lightning strikes away from equipment.
- at a proper height:
  - higher than the tallest points of objects immediately around them (such as trees, buildings, and tower legs).
  - at least 2 feet (0.6 meters) below the tallest point on the tower, pole, or roof (for lightning protection).
- in line-of-sight paths
  - to the SMs and BH.
  - that will not be obstructed by trees as they grow or structures that are later built.

NOTE:
Visual line of sight does not guarantee radio line of sight.

- away from high-RF energy sites (such as AM or FM stations, high-powered antennas, and live AM radio towers).

12.4.1 Resources for Maps and Topographic Images

Mapping software is available from sources such as the following:

- http://www.microsoft.com/streets/default.asp
  - Microsoft Streets & Trips (with Pocket Streets)
- http://www.delorme.com/software.htm
  - DeLorme Street Atlas USA
  - DeLorme Street Atlas USA Plus
  - DeLorme Street Atlas Handheld

Topographic maps are available from sources such as the following:

- http://www.delorme.com/software.htm
  - DeLorme Topo USA
  - DeLorme 3-D TopoQuads
- http://www.usgstopomaps.com
  - Timely Discount Topos, Inc. authorized maps

Topographic maps with waypoints are available from sources such as the following:

- http://www.topografix.com
  - TopoGrafix EasyGPS
  - TopoGrafix Panterra
  - TopoGrafix ExpertGPS

Topographic images are available from sources such as the following:

- http://www.keyhole.com/body.php?h=products&t=keyholePro
  - keyhole PRO
- http://www.digitalglobe.com
  - various imagery

12.4.2 Surveying Sites

Factors to survey at potential sites include

- what pre-existing wireless equipment exists at the site. (Perform spectrum analysis.)
- whether available mounting positions exist near the lowest elevation that satisfies line of site, coverage, and other link criteria.
- whether you will always have the right to decide who climbs the tower to install and maintain your equipment, and whether that person or company can climb at any hour of any day.
- whether you will have collaborative rights and veto power to prevent interference to your equipment from wireless equipment that is installed at the site in the future.
- whether a pre-existing grounding system (path to Protective Earth) exists, and what is required to establish a path to it.
- who is permitted to run any indoor lengths of cable.

12.4.3 Assuring the Essentials

In the 2.4-, 5.2-, 5.4-, and 5.7-GHz frequency band ranges, an unobstructed line of sight (LOS) must exist and be maintainable between the radios that are involved in each link.

Line of Sight (LOS) Link

In these ranges, a line of sight link is both

- an unobstructed straight line from radio to radio.
- an unobstructed zone surrounding that straight line.

Fresnel Zone Clearance

An unobstructed line of sight is important, but is not the *only* determinant of adequate placement. Even where the path has a clear line of sight, obstructions such as terrain, vegetation, metal roofs, or cars may penetrate the Fresnel zone and cause signal loss. Figure 39 illustrates an ideal Fresnel zone.

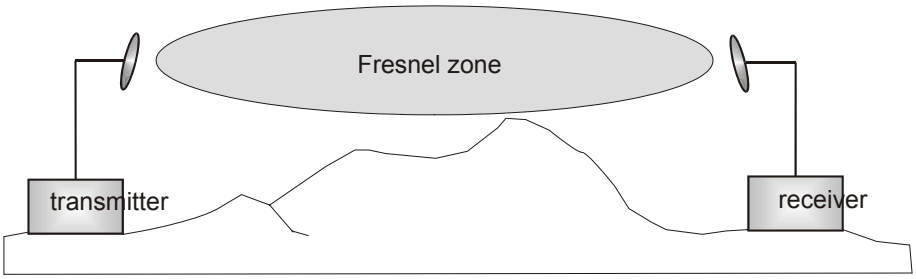


Figure 39: Fresnel zone

FresnelZoneCalcPage.xls calculates the Fresnel zone clearance that is required between the visual line of sight and the top of an obstruction that would protrude into the link path.

Non-Line of Sight (NLOS) Link

The Canopy 900-MHz modules have a line of sight (LOS) range of 40 miles (more than 64 km) and greater non-line of sight (NLOS) range than Canopy modules of other frequency bands. NLOS range depends on RF considerations such as foliage, topography, obstructions.

12.4.4 Finding the Expected Coverage Area

The transmitted beam in the vertical dimension covers more area beyond than in front of the beam center. BeamwidthRadiiCalcPage.xls calculates the radii of the beam coverage area.

12.4.5 Clearing the Radio Horizon

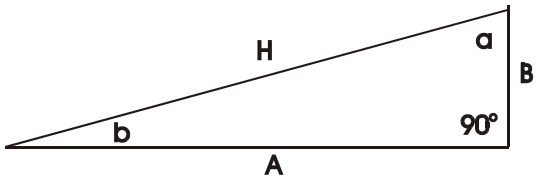
Because the surface of the earth is curved, higher module elevations are required for greater link distances. This effect can be critical to link connectivity in link spans that are greater than 8 miles (12 km). AntennaElevationCalcPage.xls calculates the minimum antenna elevation for these cases, presuming no landscape elevation difference from one end of the link to the other.

12.4.6 Calculating the Aim Angles

The appropriate angle of AP downward tilt is derived from both the distance between transmitter and receiver and the difference in their elevations. DowntiltCalcPage.xls calculates this angle.

The proper angle of tilt can be calculated as a factor of both the difference in elevation and the distance that the link spans. Even in this case, a plumb line and a protractor can be helpful to ensure the proper tilt. This tilt is typically minimal.

The number of degrees to offset (from vertical) the mounting hardware leg of the support tube is equal to the angle of elevation from the lower module to the higher module (<B in the example provided in Figure 40).



LEGEND

b	**Angle of elevation.**
B	**Vertical difference in elevation.**
A	**Horizontal distance between modules.**

Figure 40: Variables for calculating angle of elevation (and depression)

Calculating the Angle of Elevation

To use metric units to find the angle of elevation, use the following formula:

$$\tan b = \frac{B}{1000A}$$

where
B is expressed in meters
A is expressed in kilometers.

To use English standard units to find the angle of elevation, use the following formula:

$$\tan b = \frac{B}{5280A}$$

where
B is expressed in feet
A is expressed in miles.

The angle of depression from the higher module is identical to the angle of elevation from the lower module.

12.5 COLLOCATING CANOPY MODULES

Canopy APs and a BHM can be collocated at the same site *only if* the following rules are observed:

- APs are on a different frequency band range from that of the BHM or one of the following conditions applies:
  - They are vertically separated on a structure by at least 100 feet (30 m).
  - They are vertically separated on a structure by less distance, but either
    - an RF shield isolates the APs from the BHM.
    - the uplink and downlink data parameters and control channels match.
- All collocated modules are synchronized by a CMM.

Canopy APs and a BHS can be collocated at the same site only if they operate in different frequency band ranges.

12.6 DIAGRAMMING NETWORK LAYOUTS

12.6.1 Accounting for Link Ranges and Service Coverage

A 2.4-, 5,4-, or 5.7-GHz SM can be used with a Canopy Passive Reflector dish. This reflector extends the maximum span of a link as indicated in Table 28.

Table 28: Range of links with and without Passive Reflector

Modules in Link		Reflector	Typical Range[3]
SM	AP		
9000SMC (DES)	9000APC (DES)	none	40 miles (64 km)
9001SMC (AES)	9001APC (AES)	none	40 miles (64 km)
2400SM (DES)[1]	2400AP (DES)	none	5 miles (8 km)
2401SM (AES)[2]	2401AP (AES)		
2400SMRF (DES)	2400AP (DES)	on SM	15 miles (24 km)
2401SMRF (AES)	2401AP (AES)	on SM	15 miles (24 km)
5200SM (DES)	5200AP (DES)	None allowed in U.S.A or Canada	2 miles (3.2 km)
5201SM (AES)	5201AP (AES)		
5400SM (DES)	5400AP (DES)	none	2 miles (3.2 km)
5400SMRF (DES)	5400AP (DES)	on SM	10 miles (16 km)
5700SM (DES)	5700AP (DES)	none	2 miles (3.2 km)
5701SM (AES)	5701AP (AES)		
5700SMRF (DES)	5700AP (DES)	on SM	10 miles (16 km)
5701SMRF (AES)	5701AP (AES)	on SM	10 miles (16 km)

NOTES:

1. DES indicates that the module is preconfigured for Data Encryption Standard security. See Encrypting Canopy Radio Transmissions on Page 296.
2. AES indicates that the module is preconfigured for Advanced Encryption Standard security.
3. Terrain and other line of sight circumstances affect the distance that can be achieved. Additionally, local or national radio regulations may govern whether and how the Passive Reflector can be deployed.

On either or both ends of a BH link as well, a Canopy Passive Reflector dish extends the transmission and reception range as indicated in the following tables.

Table 29: Range of 2.4-GHz BH with and without Passive Reflector

Modules in Link		Data Rate	Reflectors	Typical Range
BH	BH			
2400BH (DES)	2400BH (DES)	10 Mbps	none	5 miles (8 km)
2401BH (AES)	2401BH (AES)			
2400BHRF (DES)	2400BH (DES)	10 Mbps	one end	15 miles (24 km)
2400BHRF (DES)	2400BHRF (DES)	10 Mbps	both ends	35 miles (56 km)
2401BHRF (AES)	2401BH (AES)	10 Mbps	one end	15 miles (24 km)
2401BHRF (AES)	2401BHRF (AES)	10 Mbps	both ends	35 miles (56 km)
2400BH20 (DES)	2400BH20 (DES)	20 Mbps	none	3 miles (4.8 km)
2400BHRF20 (DES)	2400BH20 (DES)	20 Mbps	one end	5 miles (8 km)
2400BHRF20 (DES)	2400BHRF20 (DES)	20 Mbps	both ends	35 miles (56 km)

Table 30: Range of 5.2-GHz BH with and without Passive Reflector

Modules in Link		Data Rate	Reflectors	Typical Range
BH	BH			
5200BH (DES)	5200BH (DES)	10 Mbps	None allowed in U.S.A or Canada	2 miles (3.2 km)
5201BH (AES)	5201BH (AES)			
5210BHRF (DES)	5210BHRF (DES)	10 Mbps	one end	2 miles (3.2 km)
5210BHRF (DES)	5210BHRF (DES)	10 Mbps	both ends	10 miles (16 km)
5210BHRF20 (DES)	5210BHRF20 (DES)	20 Mbps	one end	1 mile (1.6 km)
5210BHRF20 (DES)	5210BHRF20 (DES)	20 Mbps	both ends	5 miles (8 km)
5211BHRF (AES)	5211BHRF (AES)	10 Mbps	one end	2 miles (3.2 km)
5211BHRF (AES)	5211BHRF (AES)	10 Mbps	both ends	10 miles (16 km)

Table 31: Range of 5.4-GHz BH with and without Passive Reflector

Modules in Link		Data Rate	Reflectors	Typical Range
BH	BH			
5400BH (DES)	5400BH (DES)	10 Mbps	none	2 miles (3.2 km)
5400BHRF (DES)	5400BH (DES)	10 Mbps	one end	10 miles (16 km)
5400BHRF (DES)	5400BHRF (DES)	10 Mbps	both ends	35 miles (56 km)
5400BH20 (DES)	5400BH20 (DES)	20 Mbps	none	1 mile (1.6 km)
5400BHRF20 (DES)	5400BH20 (DES)	20 Mbps	one end	5 miles (8 km)
5400BHRF20 (DES)	5400BHRF20 (DES)	20 Mbps	both ends	35 miles (56 km)

Table 32: Range of 5.7-GHz BH with and without Passive Reflector

Modules in Link		Data Rate	Reflectors	Typical Range
BH	BH			
5700BH (DES)	5700BH (DES)	10 Mbps	none	2 miles (3.2 km)
5701BH (AES)	5701BH (AES)			
5700BHRF (DES)	5700BH (DES)	10 Mbps	one end	10 miles (16 km)
5700BHRF (DES)	5700BHRF (DES)	10 Mbps	both ends	35 miles (56 km)
5701BHRF (AES)	5701BH (AES)	10 Mbps	one end	10 miles (16 km)
5701BHRF (AES)	5701BHRF (AES)	10 Mbps	both ends	35 miles (56 km)
5700BH20 (DES)	5700BH20 (DES)	20 Mbps	none	1 mile (1.6 km)
5700BHRF20 (DES)	5700BH20 (DES)	20 Mbps	one end	5 miles (8 km)
5700BHRF20 (DES)	5700BHRF20 (DES)	20 Mbps	both ends	35 miles (56 km)

12.6.2 Accounting for Data Handling Requirements

The aggregate throughput through each AP is greater than 6 Mbps, regardless of the downlink percentage setting. This throughput includes all downlink data to all SMs and all uplink data from all SMs that link to the AP.

The downlink throughput to a single SM can be greater than 4 Mbps. The uplink throughput to an AP can be as great as approximately 2 Mbps, depending on the uplink/downlink ratio.

For 10-Mbps BHs, the aggregate throughput on the channel is 7 Mbps. For 20-Mbps BHs, the aggregate throughput on the channel is 14 Mbps. If a BH is set to a downlink ratio of 50%, then the bandwidth in each direction is half of the total BH link bandwidth.

12.6.3 Avoiding Self Interference

For 5.2-, 5.4-, and 5.7-GHz modules, 20-MHz wide channels are centered every 5 MHz. For 2.4-GHz modules, 20-MHz wide channels are centered every 2.5 MHz. This allows you to customize the channel layout for interoperability where other Canopy equipment is collocated.

CAUTION!
Regardless of whether 2.4-, 5.2-, 5.4-, or 5.7-GHz modules are deployed, channel separation between modules should be at least 20 MHz.

Physical Proximity

A BH and an AP on the same tower, or separated by less than 100 vertical feet (30 meters), require a CMM. The CMM properly synchronizes all Canopy modules to prevent interference and desensing of the modules. At closer distances without sync, the frame structures that these modules transmit and receive cause interference.

Spectrum Analysis

In Release 4.1 and later releases, you can use an SM or BHS as a spectrum analyzer. See Mapping RF Neighbor Frequencies on Page 98.

Power Reduction to Mitigate Interference

In Release 4.1 and later releases, where any module (SM, AP, BH timing master, or BH timing slave) is close enough to another module that self-interference is possible, the operator can set the SM to operate at 18 dB less than full power. The Power Control feature provides this functionality. To enable this functionality, perform the following steps.

CAUTION!
Selection of **Low** can cause a link to a distant BHS to drop. If a link drops when Power Control is set to low, the link can be re-established by only Ethernet access.

Procedure 3: Invoking the low power mode

1. Access the Configuration page of the module.
2. In the **Power Control** parameter, click **Low**.
3. Click **Save Changes**.
4. Click **Reboot**.
5. Access the Alignment page of the SM.

6. Assess whether the desired links for this module achieve
   - RSSI greater than 700.
   - jitter value between 0 and 4 in Release 4.0 and later releases or between 5 and 9 in any earlier release.
7. Access the Link Test page of the module.
8. Assess whether the desired links for this module achieve
   - uplink efficiency greater than 90%.
   - downlink efficiency greater than 90%.
9. If the desired links fail to achieve any of the above measurement thresholds, then
   a. access the module by direct Ethernet connection.
   b. access the Configuration page of the module.
   c. in the **Power Control** parameter, click **Full**.
   d. click **Save Changes**.
   e. click **Reboot**.

========== **end of procedure** ==========

12.6.4 Avoiding Other Interference

Where signal strength cannot dominate noise levels, the network experiences

- bit error corrections.
- packet errors and retransmissions.
- low throughput and high latency (because so much bandwidth is consumed by retransmissions).

Be especially cognitive of these symptoms for 900-MHz links. Where you see these symptoms, attempt the following remedies:

- Adjust the position of the SM.
- Deploy a band pass filter at the AP.
- Consider adding a remote AP closer to the affected SMs.

Certain other actions, which may seem to be potential remedies, *do not* resolve high noise level problems:

- *Do not* deploy an omnidirectional or vertically polarized antenna.
- *Do not* set the antenna gain above the recommended level.
- *Do not* deploy a band pass filter in the expectation that this can mitigate interband interference.

13 ENGINEERING YOUR IP COMMUNICATIONS

13.1 UNDERSTANDING ADDRESSES

A basic understanding of Internet Protocol (IP) address and subnet mask concepts is required for engineering your IP networking.

13.1.1 IP Address

The IP address is a 32-bit binary number that has four parts (octets). This set of four octets has two segments, depending on the class of IP address. The first segment identifies the network. The second identifies the hosts or devices on the network. The subnet mask marks a boundary between these two sub-addresses.

13.2 DYNAMIC OR STATIC ADDRESSING

For any computer to communicate with a Canopy module, the computer must be configured to either

- use DHCP (Dynamic Host Configuration Protocol). In this case, when not connected to the network, the computer derives an IP address on the 169.254 network within two minutes.
- have an assigned static IP address (for example, 169.254.1.5) on the 169.254 network.

IMPORTANT!
If an IP address that is set in the module is not the 169.254.x.x network address, then the network operator must assign the computer a static IP address in the same subnet.

13.2.1 When a DHCP Server is Not Found

The following is a synopsis of an Internet Draft available at http://www.ietf.org/internet-drafts/draft-ietf-zeroconf-ipv4-linklocal-05.txt. This draft describes how Microsoft and Apple operating systems react when a DHCP server is not found on the network.

To operate on a network, a computer requires an IP address, a subnet mask, and possibly a gateway address. Either a DHCP server automatically assigns this configuration information to a computer on a network or an operator must input these items.

When a computer is brought online and a DHCP server is not accessible (such as when the server is down or the computer is not plugged into the network), Microsoft and Apple operating systems default to an IP address of 169.254.x.x and a subnet mask of 255.255.0.0 (169.254/16, where /16 indicates that the first 16 bits of the address range are identical among all members of the subnet).

13.3 NETWORK ADDRESS TRANSLATION (NAT)

13.3.1 NAT, DHCP Server, DHCP Client, and DMZ in SM

In Release 4.1 and later releases, the Canopy system provides NAT (network address translation for SMs in the following combinations of NAT and DHCP (Dynamic Host Confiuration Protocol):

- NAT Disabled (as in earlier releases)
- NAT with DHCP Client and DHCP Server
- NAT with DHCP Client
- NAT with DHCP Server
- NAT without DHCP

NAT

NAT isolates the SMs from the Internet. This both enhances SM security and obviates the need for a special assignment scheme of IP addresses that identify the SMs. Where NAT is active, the SM serves as a Layer 3 switch. (By contrast, where NAT is not active, the SM serves as a Layer 2 bridge.)

In the Canopy system, NAT supports HTTP, ICMP (Internet Control Message Protocols), and FTP (File Transfer Protocol), but *does not* support IPsec (IP Secure) except as described under NAT Pass-through of VPN as L2TP over IPSec on Page 122.

DHCP

DHCP enables a device to be assigned a new IP address and TCP/IP parameters, including a default gateway, whenever the device reboots. Thus DHCP reduces configuration time, conserves IP addresses, and allows modules to be moved to a different network within the Canopy system.

In conjunction with the NAT features, each SM provides

- a DHCP server that assigns IP addresses to computers connected to the SM by Ethernet protocol.
- a DHCP client that receives an IP address for the SM from a network DHCP server.

DMZ

In conjunction with the NAT features, a DMZ (demilitarized zone) allows the assignment of one IP address behind the SM for a device to logically exist outside the firewall and receive network traffic. The first three octets of this IP address must be identical to the first three octets of the NAT private IP address.

NAT Disabled

The NAT Disabled implementation is illustrated in Figure 41.

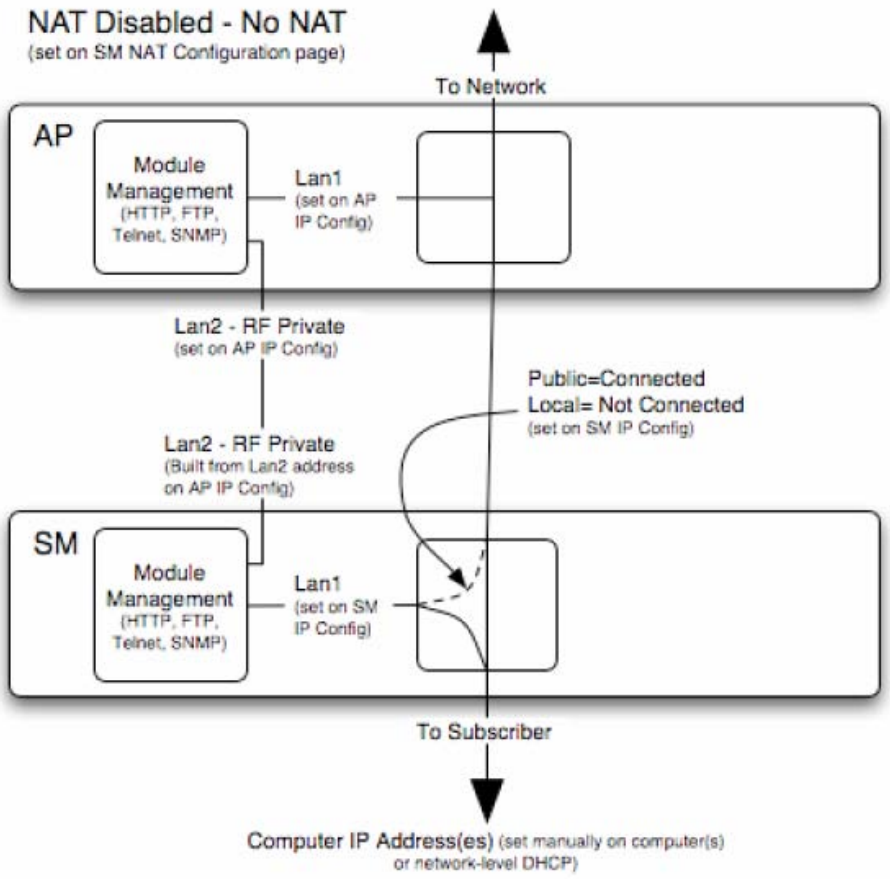

NAT Disabled - No NAT
(set on SM NAT Configuration page)
To Network
AP
Module Management (HTTP, FTP, Telnet, SNMP)
Lan1 (set on AP IP Config)
Lan2 - RF Private (set on AP IP Config)
Public=Connected
Local= Not Connected
(set on SM IP Config)
Lan2 - RF Private (Built from Lan2 address on AP IP Config)
SM
Module Management (HTTP, FTP, Telnet, SNMP)
Lan1 (set on SM IP Config)
To Subscriber
Computer IP Address(es) (set manually on computer(s) or network-level DHCP)

Figure 41: NAT Disabled implementation

This implementation is provisioned as displayed in

- Figure 77 on Page 215 and Figure 78 on Page 216.
- Figure 83 on Page 223.

NAT with DHCP Client and DHCP Server

The NAT with DHCP Client and DHCP Server implementation is illustrated in Figure 42.

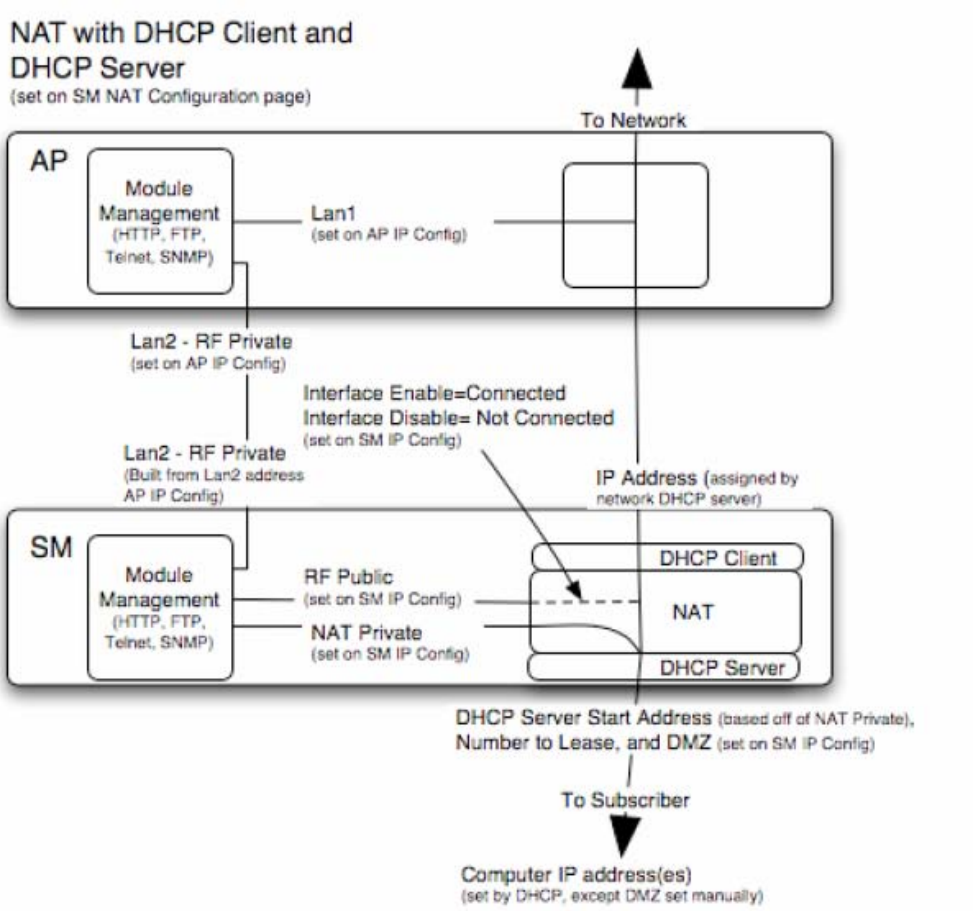


Figure 42: NAT with DHCP Client and DHCP Server implementation

This implementation is provisioned as displayed in Figure 79 on Page 218 and Figure 85 on Page 227.

NAT with DHCP Client

The NAT with DHCP Client implementation is illustrated in Figure 43.

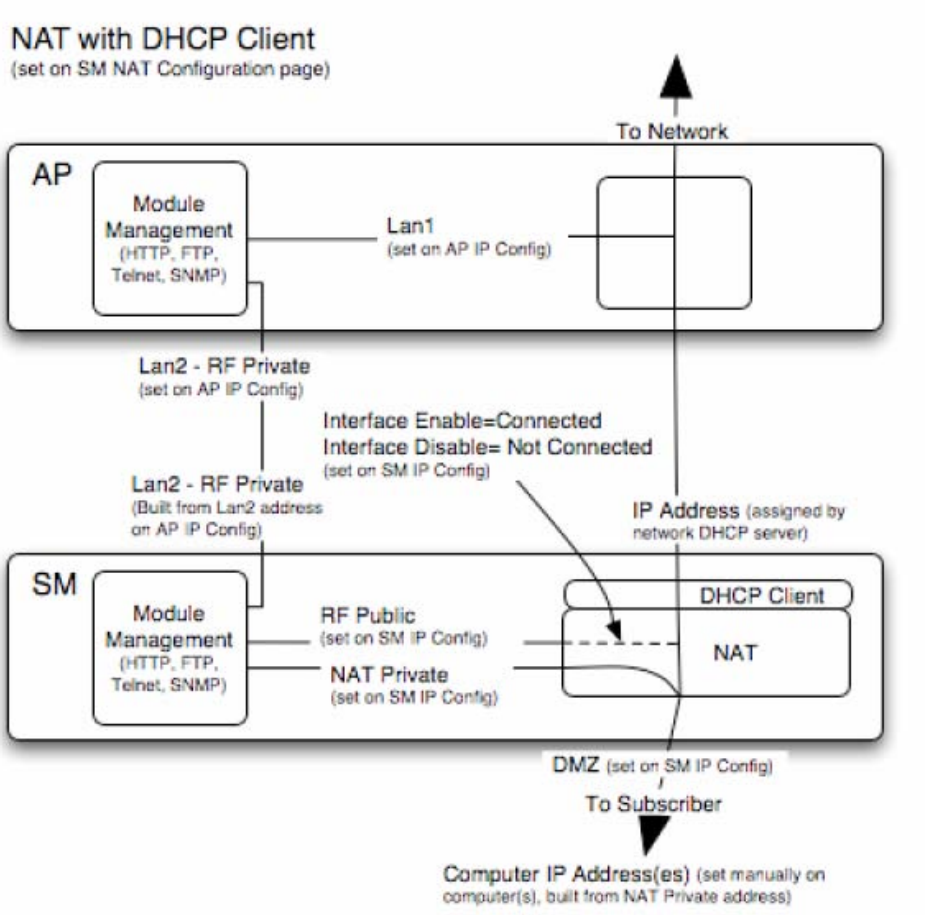

NAT with DHCP Client
(set on SM NAT Configuration page)
To Network
AP
Module Management (HTTP, FTP, Telnet, SNMP)
Lan1
(set on AP IP Config)
Lan2 - RF Private
(set on AP IP Config)
Interface Enable=Connected
Interface Disable= Not Connected
(set on SM IP Config)
Lan2 - RF Private
(Built from Lan2 address on AP IP Config)
IP Address (assigned by network DHCP server)
SM
Module Management (HTTP, FTP, Telnet, SNMP)
RF Public
(set on SM IP Config)
NAT Private
(set on SM IP Config)
DHCP Client
NAT
DMZ (set on SM IP Config)
To Subscriber
Computer IP Address(es) (set manually on computer(s), built from NAT Private address)

Figure 43: NAT with DHCP Client implementation

This implementation is provisioned as displayed in Figure 80 on Page 219 and Figure 86 on Page 228.

NAT with DHCP Server

The NAT with DHCP Server implementation is illustrated in Figure 44.

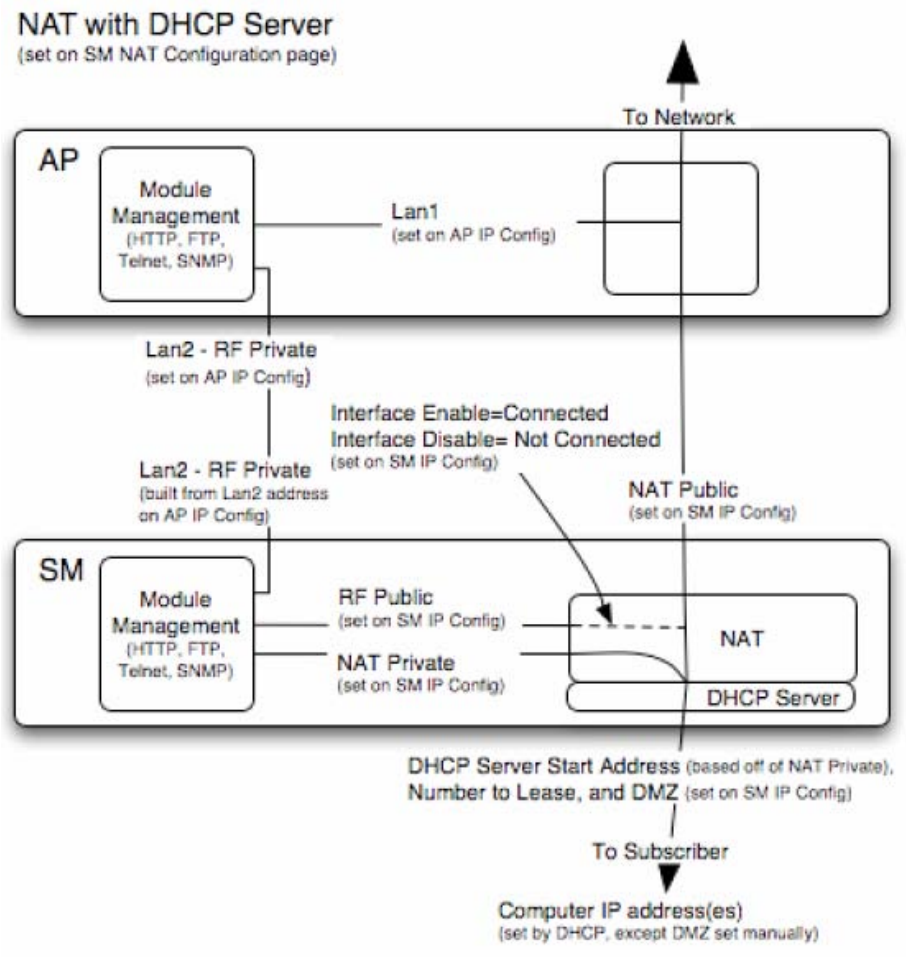

NAT with DHCP Server
(set on SM NAT Configuration page)
To Network
AP
Module Management
(HTTP, FTP, Telnet, SNMP)
Lan1
(set on AP IP Config)
Lan2 - RF Private
(set on AP IP Config)
Interface Enable=Connected
Interface Disable= Not Connected
(set on SM IP Config)
Lan2 - RF Private
(built from Lan2 address on AP IP Config)
NAT Public
(set on SM IP Config)
SM
Module Management
(HTTP, FTP, Telnet, SNMP)
RF Public
(set on SM IP Config)
NAT Private
(set on SM IP Config)
NAT
DHCP Server
DHCP Server Start Address (based off of NAT Private), Number to Lease, and DMZ (set on SM IP Config)
To Subscriber
Computer IP address(es)
(set by DHCP, except DMZ set manually)

Figure 44: NAT with DHCP Server implementation

This implementation is provisioned as displayed in Figure 81: IP Configuration screen, NAT with DHCP server on Page 220 and Figure 87: NAT Configuration screen, NAT with DHCP server on Page 229.

NAT without DHCP

The NAT without DHCP implementation is illustrated in Figure 45.

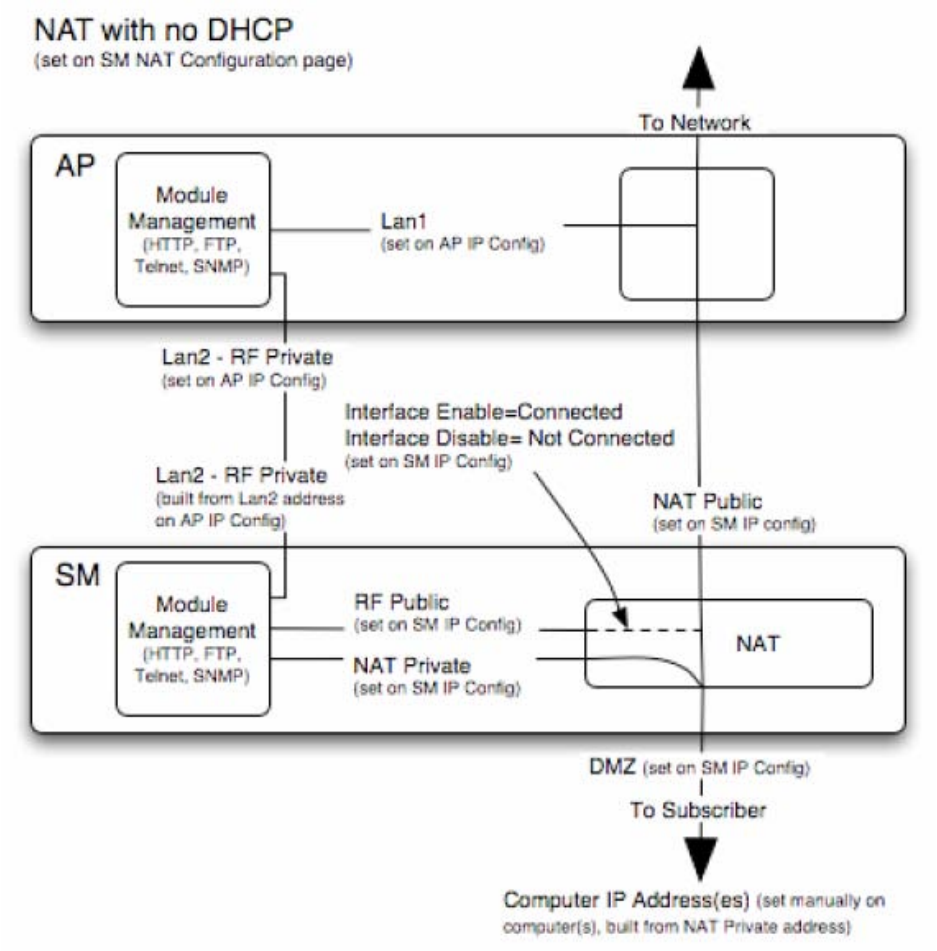

NAT with no DHCP
(set on SM NAT Configuration page)
To Network
AP
Module Management (HTTP, FTP, Telnet, SNMP)
Lan1 (set on AP IP Config)
Lan2 - RF Private (set on AP IP Config)
Interface Enable=Connected
Interface Disable= Not Connected
(set on SM IP Config)
Lan2 - RF Private (built from Lan2 address on AP IP Config)
NAT Public (set on SM IP config)
SM
Module Management (HTTP, FTP, Telnet, SNMP)
RF Public (set on SM IP Config)
NAT Private (set on SM IP Config)
NAT
DMZ (set on SM IP Config)
To Subscriber
Computer IP Address(es) (set manually on computer(s), built from NAT Private address)

Figure 45: NAT without DHCP implementation

This implementation is provisioned as displayed in Figure 82: IP Configuration screen, NAT without DHCP on Page 221 and Figure 88: NAT Configuration screen, NAT without DHCP on Page 230.

13.3.2 NAT Pass-through of VPN as L2TP over IPSec

Release 4.1 introduced NAT on Canopy SMs, but *does not* support NAT pass-through of Virtual Private Networks (VPNs).

The latest operating systems from Microsoft (Windows XP) and Apple (Panther) provide an option to select either L2TP over IPSec (Level 2 Tunneling Protocol over IP Security, the most popular VPN implementation) or PPTP (Point to Point Tunneling Protocol) for a

VPN. Release 4.2 and later releases support NAT passing L2TP over IPSec but *do not* support NAT passing PPTP. When one of these later releases is installed in the SM, NAT Pass-through of VPN as L2TP over IPSec is enabled with no required further provisioning.

13.4 DEVELOPING AN IP ADDRESSING SCHEME

Canopy network elements are accessed through IP Version 4 (IPv4) addressing. A proper IP addressing method is critical to the operation and security of a Canopy network.

Each Canopy module requires an IP address on the network. This IP address is for only management purposes. For security, you should either

- assign an unroutable IP address.
- assign a routable IP address only if a firewall is present to protect the module.

You will assign IP addresses to computers and network components by either *static* or *dynamic* IP addressing. You will also assign the appropriate subnet mask and network gateway to each module.

13.4.1 Address Resolution Protocol

As previously stated, the MAC address identifies a Canopy module in

- communications between modules.
- the data that modules store about each other.
- the data that the BAM software applies to manage authentication and bandwidth.

The IP address is essential for data delivery through a router interface. Address Resolution Protocol (ARP) correlates MAC addresses to IP addresses.

For communications to outside the network segment, ARP reads the network gateway address of the router and translates it into the MAC address of the router. Then the communication is sent to MAC address (physical network interface card) of the router.

For each router between the sending module and the destination, this sequence applies. The ARP correlation is stored until the ARP cache times out.

13.4.2 Allocating Subnets

The subnet mask is a 32-bit binary number that filters the IP address. Where a subnet mask contains a bit set to 1, the corresponding bit in the IP address is part of the network address.

Example IP Address and Subnet Mask

In Figure 46, the first 16 bits of the 32-bit IP address identify the network:

	Octet 1	Octet 2	Octet 3	Octet 4
IP address 169.254.1.1	10101001	11111110	00000001	00000001
Subnet mask 255.255.0.0	11111111	11111111	00000000	00000000

Figure 46: Example of IP address in Class B subnet

In this example, the network address is 169.254, and 2^{16} (65,536) hosts are addressable.

13.4.3 Selecting Non-routable IP Addresses

The factory default assignments for Canopy network elements are

- unique MAC address
- IP address of 169.254.1.1
- subnet mask of 255.255.0.0
- network gateway address of 169.254.0.0

For each Canopy radio and CMMmicro, assign an IP address that is both consistent with the IP addressing plan for your network and cannot be accessed from the Internet. IP addresses within the following ranges are not routable from the Internet (regardless of whether a firewall is configured:

- 10.0.0.0 – 10.255.255.255
- 172.16.0.0 – 172.31.255.255
- 192.168.0.0 – 192.168.255.255
- 169.254.0.0 – 169.254.255.255

You can also assign a subnet mask and network gateway for each CMMmicro.

14 ENGINEERING VLANS

In Canopy System Release 6.0 and later releases, Canopy radios support VLAN functionality as defined in the 802.1Q specification, except for the following aspects of that specification:

- the following protocols:
  - GARP GARV
  - STP
  - MSTP
  - GARP GMRP
- priority encoding (802.1P)
- embedded source routing (ERIF) in the 802.1Q header
- multicast pruning
- flooding unknown unicast frames in the downlink

As an additional exception, the Canopy AP *does not* flood downward the unknown unicast frames to the Canopy SM.

A VLAN configuration in Layer 2 establishes a logical group within the network. Each computer in the VLAN, regardless of initial or eventual physical location, has access to the same data. For the network operator, this provides flexibility in network segmentation, simpler management, and enhanced security.

With the supported VLAN functionality, Canopy radios determine bridge forwarding on the basis of not only the destination MAC address, but also the VLAN ID of the destination. This provides flexibility in how SMs are used:

- Each SM can be a member in its own VLAN, whose other members can be APs in other sectors. This case would allow movement of the SM from sector to sector without requiring a reconfiguration of the VLAN.
- Each SM can be in its own broadcast domain, such that only the radios that are members of the VLAN can see multicast traffic to and from the SM. In most cases, this can significantly conserve bandwidth at the SMs.
- The network operator can define a work group of SMs, regardless of the AP in which they register.

BUILDING YOUR CANOPY NETWORK

15 AVOIDING HAZARDS

Use simple precautions to protect staff and equipment. Hazards include exposure to RF waves, lightning strikes, and power surges. This section specifically recommends actions to abate these hazards.

15.1 PREVENTING OVEREXPOSURE TO RF ENERGY

To protect from overexposure to RF energy, install Canopy radios so as to provide and maintain the minimum separation distances from all persons shown in Table 33.

Table 33: Exposure separation distances

Canopy module	Minimum separation distance from all persons	
Antenna of 900-MHz AP or SM	60 cm	24 in
2.4-, 5.2-, 5.4-, or 5.7-GHz radio with no reflector	20 cm	8 in
2.4-, 5.2-, 5.4-, or 5.7-GHz radio with a reflector	1.5 m	60 in (5 ft)

At these and greater separation distances, the power density from the RF field is below generally-accepted limits for the general population.

I

NOTE:
These are conservative distances that include compliance margins. In the case of the reflector, the distance is even more conservative because the equation used models the reflector as a point source and ignores its physical dimensions.

15.1.1 Details of Calculations for Separation Distances and Power Compliance Margins

Limits and guidelines for RF exposure come from:

- US FCC limits for the general population. See the FCC web site at http://www.fcc.gov, and the policies, guidelines, and requirements in Part 1 of Title 47 of the Code of Federal Regulations, as well as the guidelines and suggestions for evaluating compliance in FCC OET Bulletin 65.
- Health Canada limits for the general population. See the Health Canada web site at http://www.hc-sc.gc.ca/rpb and Safety Code 6.
- ICNIRP (International Commission on Non-Ionizing Radiation Protection) guidelines for the general public. See the ICNIRP web site at http://www.icnirp.de/ and Guidelines for Limiting Exposure to Time-Varying Electric, Magnetic, and Electromagnetic Fields.

The applicable power density exposure limits from the documents referenced above are

- 6 W/m^2 for RF energy in the 900-MHz frequency band in the US and Canada.
- 10 W/m^2 for RF energy in the 2.4-, 5.2-, 5.4-, and 5.7-GHz frequency bands.

Peak power density in the far field of a radio frequency point source is calculated as follows:

$$S = \frac{P \cdot G}{4 \pi d^2}$$

where
S = power density in W/m^2
P = RMS transmit power capability of the radio, in W
G = total Tx gain as a factor, converted from dB
d = distance from point source, in m

Rearranging terms to solve for distance gives

$$d = \sqrt{\frac{P \cdot G}{4 \pi S}}$$

Calculated Distances and Power Compliance Margins

TBL shows calculated minimum separation distances d, recommended distances and resulting power compliance margins for each frequency band and antenna combination.

Table 34: Power Compliance Margins

Frequency Band	Antenna	Variable			d[1]	Recommended Distance	Power Compliance Margin
		P	*G*	S			
900 MHz	external	0.4 W (26 dBm)	10.0 (10 dB)	6 W/m^2	0.23 m	60 cm (24 in)	7
2.4 GHz	internal	0.34 W (25 dBm)	6.3 (8 dB)	10 W/m^2	0.13 m	20 cm (8 in)	2.3
	internal + reflector	0.34 W (25 dBm)	79.4 (19 dB)	10 W/m^2	0.46 m	1.5 m (5 ft)	10
5.2 GHz	internal	0.2 W (23 dBm)	5.0 (7 dB)	10 W/m^2	0.09 m	20 cm (8 in)	5
	internal + reflector	0.0032 W (5 dBm)	316 (25 dB)	10 W/m^2	0.09 m	1.5 m (5 ft)	280

Frequency Band	Antenna	Variable			d^1	Recommended Distance	Power Compliance Margin
		P	*G*	S			
5.4 GHz	internal	0.2 W (23 dBm)	5.0 (7 dB)	10 W/m^2	0.09 m	20 cm (8 in)	5
	internal + reflector	0.0032 W (5 dBm)	316 (25 dB)	10 W/m^2	0.09 m	1.5 m (5 ft)	280
5.7 GHz	internal	0.2 W (23 dBm)	5.0 (7 dB)	10 W/m^2	0.09 m	20 cm (8 in)	5
	internal + reflector	0.2 W (23 dBm)	316 (25 dB)	10 W/m^2	0.71 m	1.5 m (5 ft)	4.5

NOTES:
1. Calculated.

15.2 REDIRECTING LIGHTNING STRIKES

To protect both your staff and your equipment, implement lightning protection as follows:

- Observe all local and national codes that apply to grounding for lightning protection.
- Install your modules at least 2 feet (0.6 meters) below the tallest point on the tower, pole, or roof.
- Install lightning arrestors to transport lightning strikes away from equipment. For example, install a lightning rod on a tower leg other than the leg to which you mount your module.
- Connect your lightning rod to ground.
- Use a Canopy Surge Suppressor on the Ethernet cable
  - at each interval along the tower leg.
  - where the cable enters any structure. (Instructions for installing a Canopy Surge Suppressor are provided in Procedure 32 on Page 271.)

15.3 CONFORMING TO REGULATIONS

Ensure that your network conforms to applicable country and local codes, such as the NEC (National Electrical Code) in the U.S.A. If you are uncertain of code requirements, engage the services of a licensed electrician.

15.4 PROTECTING CABLES AND CONNECTIONS

Wind

Cables that move in the wind can be damaged, impart vibrations to the connected device, or both. At installation time, prevent these problems by securing all cables with cable ties, cleats, or PVC tape.

Moisture

Over time, moisture can cause a cable connector to fail. You can prevent this problem by

- using cables that are filled with a dielectric gel or grease.
- including a drip loop where the cable approach to the module (typically a CMM2 or CMMmicro) is from above.
- wrapping the cable with weather-resistant tape.

On modules with connectorized antenna, use accepted industry practices to wrap the connector to prevent water ingress. Although the male and female N-type connectors form a gas-tight seal with each other, the point where the cable enters each connector can allow water ingress and eventual corrosion. Wrapping and sealing is critical to long-term reliability of the connection.

Possible sources of material to seal that point include

- the antenna manufacturer (material may have been provided in the package with the antenna).
- Universal Electronics (whose web site is http://www.coaxseal.com), who markets a weather-tight wrap named Coax-Seal.

Perform the following steps to wrap the cable.

Procedure 4: Wrapping the cable

1. Start the wrap on the cable 0.5 to 2 inches (about 1.5 to 5 cm) from the connection.
2. Wrap the cable to a point 0.5 to 2 inches (about 1.5 to 5 cm) above the connection.
3. Squeeze the wrap to compress and remove any trapped air.
4. Wrap premium vinyl electrical tape over the first wrap where desired for abrasion resistance or appearance.
5. Tie the cable to minimize sway from wind.

end of procedure

16 TESTING THE COMPONENTS

Before you install any component into your Canopy network, allow yourself the opportunity to discover that the component is defective. If you always follow the preliminary steps in this section, you will save

- installation and removal costs for a component that will not function.
- time in the process of replacing the defective component.

The best practice is to connect all the components—BHs, APs, GPS antenna, and CMM2 or CMMmicro—in a test setting and configure and verify them before deploying them to an installation. However, circumstances or local practice may require a different practice. In this case, appropriately modify the following procedures.

16.1 UNPACKING COMPONENTS

When you receive Canopy products, carefully inspect all shipping boxes for signs of damage. If you find damage, immediately notify the transportation company.

As you unpack the equipment, verify that all the components that you ordered have arrived. Save all the packing materials to use later, as you transport the equipment to and from installation sites.

16.2 CONFIGURING FOR TEST

You can use either of two methods to configure an AP or BHM:

- Use the Quick Start feature of the product. For more information on Quick Start, see Quick Start Page of the AP on Page 139.
- Manually set each parameter.

After you change any configuration parameter, to put the change into effect, you must do both of the following:

1. Click the **Save** button to temporarily save the change(s).
2. Click the **Reboot** button to reboot the module and implement the change(s).

16.2.1 Configuring the Computing Device for Test

If your computer is configured for Dynamic Host Configuration Protocol (DHCP), disconnect the computer from the network. If your computer is alternatively configured for static IP addressing

- set the static address in the 169.254 network
- set the subnet mask to 255.255.0.0.

16.2.2 Default Module Configuration

From the factory, the Canopy AP, SM, and BH are all configured to *not transmit* on any frequency. This configuration ensures that you do not accidentally turn on an unsynchronized module. Site synchronization of modules is required because

- Canopy modules
  - cannot transmit and receive signals at the same time.
  - use TDD (Time Division Duplexing) to distribute signal access of the downlink and uplink frames.
- when one module transmits while an unintended module nearby receives signal, the transmitting module may interfere with or desense the receiving module. In this context, interference is self-interference (within the same Canopy network).

16.2.3 Component Layout

As shown in Figure 47, the base cover of the module snaps off when you depress a lever on the back of the base cover. This exposes the Ethernet and GPS sync connectors and diagnostic LEDs.

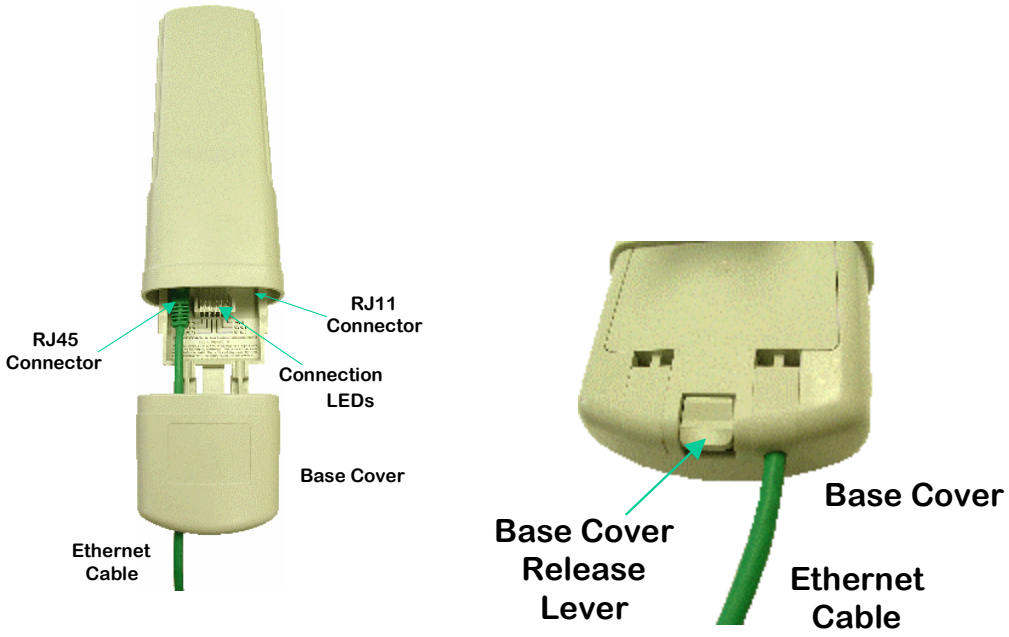


Figure 47: Canopy base cover, attached and detached

16.2.4 Diagnostic LEDs

The diagnostic LEDs report the following information about the status of the module. Table 35 and Table 36 identify the LEDs in order of their left-to-right position as the cable connections face downward.

NOTE:
The LED color helps you distinguish position of the LED. The LED color *does not* indicate any status.

Table 35: LEDs in AP and BHM

Label	Color when Active	Status Information Provided	Notes
LNK/5	green	Ethernet link	Continuously lit when link is present.
ACT/4	orange	Presence of data activity on the Ethernet link	Flashes during data transfer. Frequency of flash is not a diagnostic indication.
GPS/3	red	Pulse of sync	Continuously lit as pulse as AP receives pulse.
SES/2	green	*Unused on the AP*	SES is the session indicator on the CMM.
SYN/1	orange	Presence of sync	Always lit on the AP.
PWR	red	DC power	Always lit when power is correctly supplied.

Table 36: LEDs in SM and BHS

Label	Color when Active	Status if Registered	Notes	
			Operating Mode	Aiming Mode
LNK/5	green	Ethernet link	Continuously lit when link is present.	These five LEDs act as a bar graph to indicate the relative quality of alignment. As RSSI (received signal strength indicator) and jitter improve during alignment, more of these LEDs are lit.
ACT/4	orange	Presence of data activity on the Ethernet link	Flashes during data transfer. Frequency of flash is not a diagnostic indication.	
GPS/3	red	*Unused*	If this module is not registered to another, then these three LEDs cycle on and off from left to right.	
SES/2	green	*Unused*		
SYN/1	orange	Presence of sync		
PWR	red	DC power	Always lit when power is correctly supplied.	Always lit when power is correctly supplied.

16.2.5 CMM2 Component Layout

As shown in Figure 103 on Page 266, the CMM2 comprises four assemblies:

- Ethernet switch
- Power transformer
- Interconnect board
- GPS receiver.

Some CMM2s that were sold earlier had four openings in the bottom plate, as shown in Figure 48. Currently available CMM2s have two *additional* Ethernet cable and GPS sync cable openings to allow use of thicker, shielded cables.

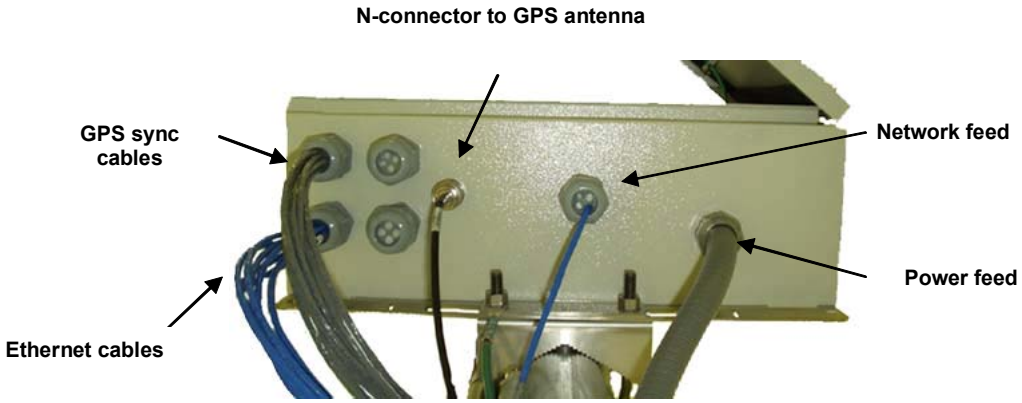
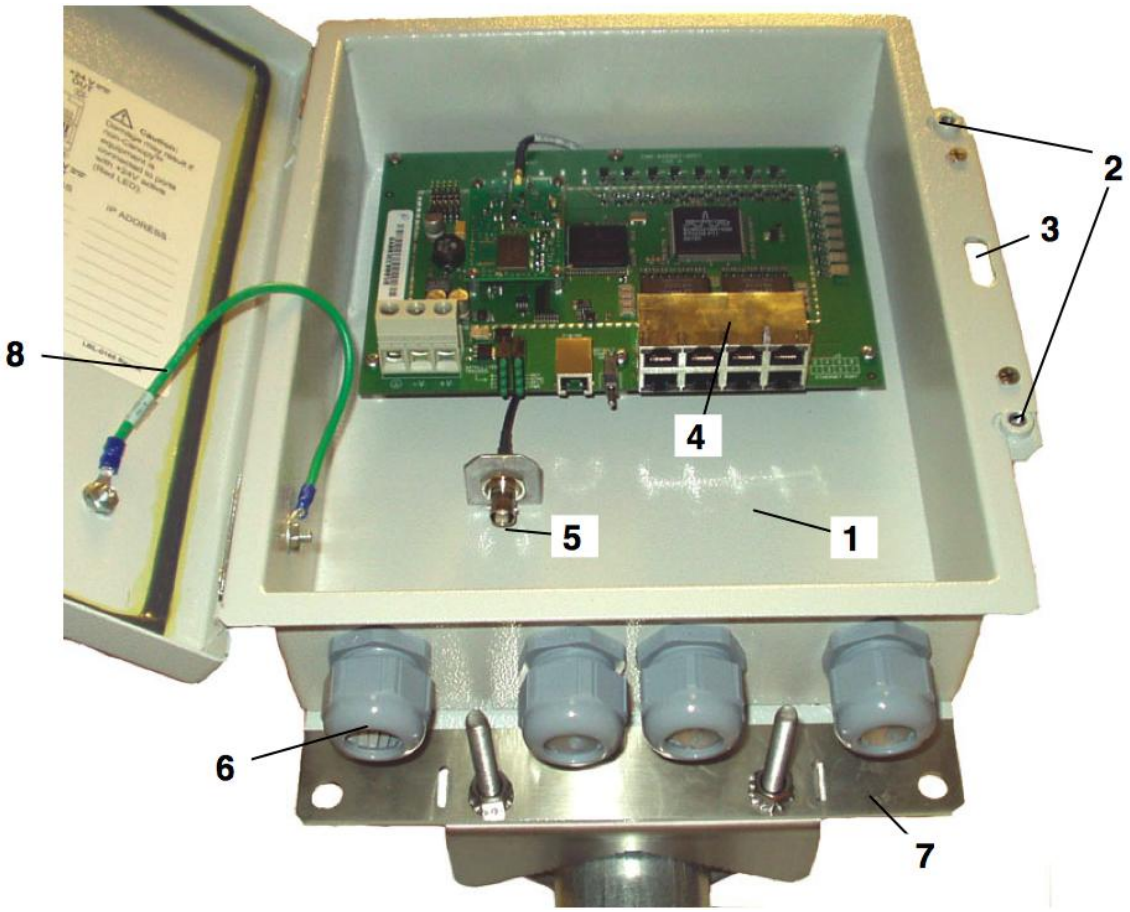


Figure 48: Canopy CMM2, bottom view

16.2.6 CMMmicro Component Layout

The layout of the CMMmicro is shown in Figure 49.



LEGEND

1. Weatherized enclosure
2. Thumb-screw/slot-screwdriver door fasteners
3. Punch-out for padlock
4. Ethernet switch and power module
5. Female BNC connector
6. Water-tight bulkhead connectors
7. Flange for attachment (stainless steel for grounding to tower or building) using U bolts (provided) or other hardware such as screws, lag bolts, or attachment straps (not provided)
8. Ground strap (for grounding door to enclosure)
9. 100-W 115/230-V AC to 24-V DC power converter, with 10 ft (3 m) of DC power cable (not shown)
10. 6-ft (1.8-m) AC power cord for 24 V power converter (not shown)

Figure 49: Cluster Management Module micro

16.2.7 Standards for Wiring

Canopy modules that are currently available automatically sense whether the Ethernet cable in a connection is wired as straight-through or crossover. You may use either straight-through or crossover cable to connect a network interface card (NIC), hub, router, or switch to these modules. For a straight-through cable, use the EIA/TIA-568B wire color-code standard on both ends. For a crossover cable, use the EIA/TIA-568B wire color-code standard on one end, and the EIA/TIA-568A wire color-code standard on the other end.

Some modules that were sold earlier do not automatically sense the wiring scheme. To identify whether an older module senses the Ethernet cable type, compare the ESN of the module to the ESNs listed in Table 37.

Table 37: Cable scheme auto-sensing per MAC address

Module Type	MAC Address (ESN) of Non Auto-sensing Module	MAC Address (ESN) of Auto-Sensing Module
900-MHz, 2.4-GHz, and 5.4-GHz modules	(no ESNs)	(all ESNs)
5.2-GHz Modules	≤ 0A003E0021C8	≥ 0A003E0021C9
5.7-GHz Modules	≤ 0A003EF00F79	≥ 0A003EF00F79A

CAUTION!

Where you use a *non* auto-sensing module

- use a straight-through cable to connect to a NIC (network interface card).
- use a crossover cable to connect to a hub, switch, or router.

Where you use the Canopy AC wall adapter

- the +V is +11.5 VDC to +30 VDC, with a nominal value of +24 VDC.
- the maximum Ethernet cable run is 328 feet (100 meters).

16.2.8 Best Practices for Cabling

The following practices are essential to the reliability and longevity of cabled connections:

- Use only shielded cables to resist interference.
- For vertical runs, provide cable support and strain relief according to applicable regulations.
- Include a 2-ft (0.6-m) service loop on each end of the cable to allow for thermal expansion and contraction and to facilitate terminating the cable again when needed.
- Ensure that all connections are properly crimped.

- Use dielectric grease on all connectors to resist corrosion.
- Use only shielded connectors to resist interference and corrosion.

16.2.9 Recommended Tools for Wiring Connectors

The following tools may be needed for cabling the AP:

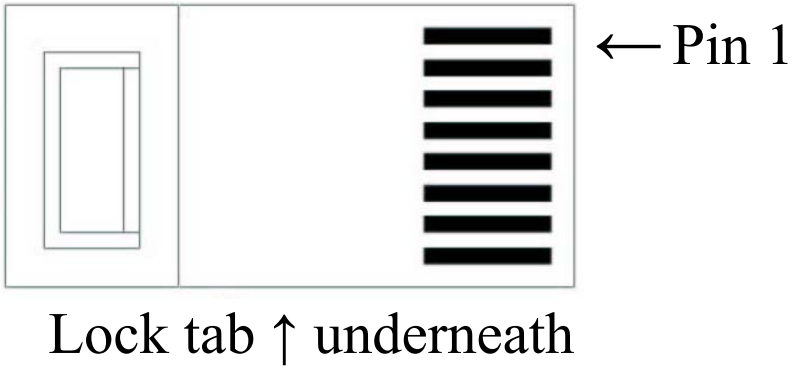
- RJ-11 crimping tool
- RJ-45 crimping tool
- electrician scissors
- wire cutters
- cable testing device.

16.2.10 Wiring Connectors

The following diagrams correlate pins to wire colors and illustrate crossovers where applicable.

Location of Pin 1

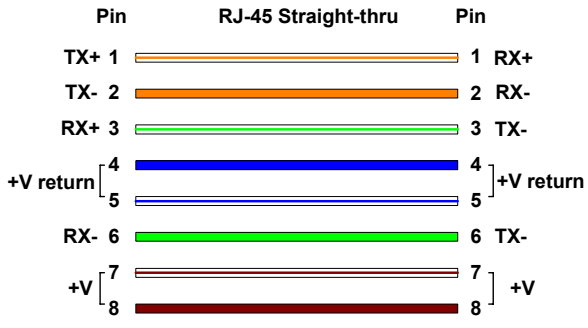
Pin 1, relative to the lock tab on the connector of a straight-through cable is located as shown below.



RJ-45 Pinout for Straight-through Ethernet Cable

Pin 1 →	white / orange	← Pin 1
Pin 2 →	orange	← Pin 2
Pin 3 →	white / green	← Pin 3
Pin 4 →	blue	← Pin 4
Pin 5 →	white / blue	← Pin 5
Pin 6 →	green	← Pin 6
Pin 7 →	white / brown	← Pin 7
Pin 8 →	brown	← Pin 8

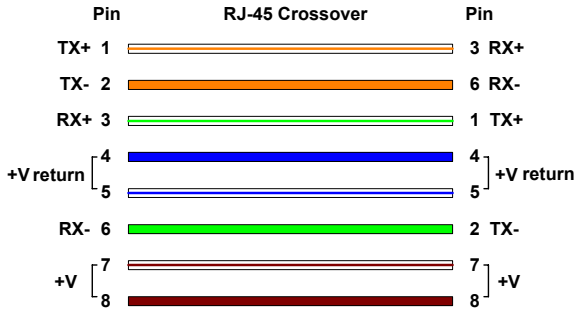
Pins 7 and 8 carry power to the modules.



RJ-45 Pinout for Crossover Ethernet Cable

Pin 1 →	white / orange	← Pin 3
Pin 2 →	orange	← Pin 6
Pin 3 →	white / green	← Pin 1
Pin 4 →	blue	← Pin 4
Pin 5 →	white / blue	← Pin 5
Pin 6 →	green	← Pin 2
Pin 7 →	white / brown	← Pin 7
Pin 8 →	brown	← Pin 8

Pins 7 and 8 carry power to the modules.

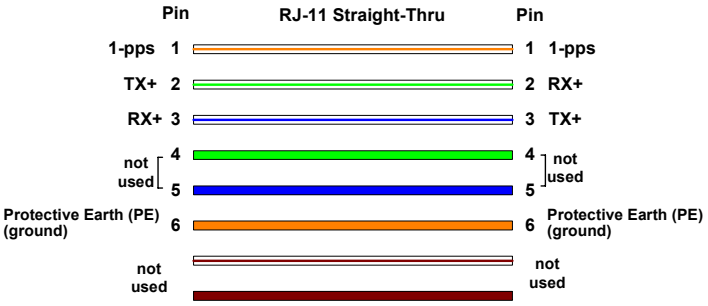


RJ-11 Pinout for Straight-through Sync Cable

An RJ-11 connectors are commonly used to connect a devices to phone lines. The Canopy system uses a utility cable with RJ-11 connectors between the AP or BH and synchronization pulse. Presuming CAT 5 cable and 6-pin RJ-11 connectors, the following diagram shows the wiring of the cable for sync.

Pin 1 → white / orange ← Pin 1
Pin 2 → white / green ← Pin 2
Pin 3 → white / blue ← Pin 3
Pin 4 → green ← Pin 4
Pin 5 → blue ← Pin 5
Pin 6 → orange ← Pin 6

NOTE: The fourth pair is not used.



16.3 CONFIGURING A POINT-TO-MULTIPOINT LINK FOR TEST

Perform the following steps to begin the test setup.

Procedure 5: Setting up the AP for Quick Start

1. In one hand, securely hold the top (larger shell) of the AP. With the other hand, depress the lever in the back of the base cover (smaller shell). Remove the base cover.
2. Plug one end of a CAT 5 Ethernet cable into the AP.
3. Plug the other end of the Ethernet cable into the jack in the pig tail that hangs from the power supply.

WARNING!
From this point until you remove power from the AP, stay at least as far from the AP as the minimum separation distance specified under Preventing Overexposure to RF on Page 127.

4. Plug the other connector of the pig tail into the Ethernet jack of the computing device.
5. Plug the power supply into an electrical outlet.
6. Power up the computing device.
7. Start the browser in the computing device.

end of procedure

The Canopy AP interface provides a series of web pages to configure and monitor the unit. These screens are subject to change by subsequent software releases.

You can access the web-based interface through a computing device that is either directly connected or connected through a network to the AP. If the computing device is not connected to a network when you are configuring the module in your test environment, and if the computer has used a proxy server address and port to configure a Canopy module, then you may need to first disable the proxy setting in the computer.

Perform the following procedure to toggle the computer to *not* use the proxy setting.

Procedure 6: Bypassing proxy settings to access module web pages

1. Launch Microsoft Internet Explorer.
2. Select **Tools** → **Internet Options** → **Connections** → **LAN Settings**.
3. Uncheck the **Use a proxy server…** box.
   NOTE: If you use an alternate web browser, the menu selections differ from the above.

end of procedure

In the address bar of your browser, enter the IP address of the AP (default is 169.254.1.1). The AP responds by opening the Status page.

16.3.1 Quick Start Page of the AP

To proceed with the test setup, click the **Quick Start** button on the left side of the Status page. The AP responds by opening the Quick Start page. The standard Quick Start screen is displayed in Figure 50.

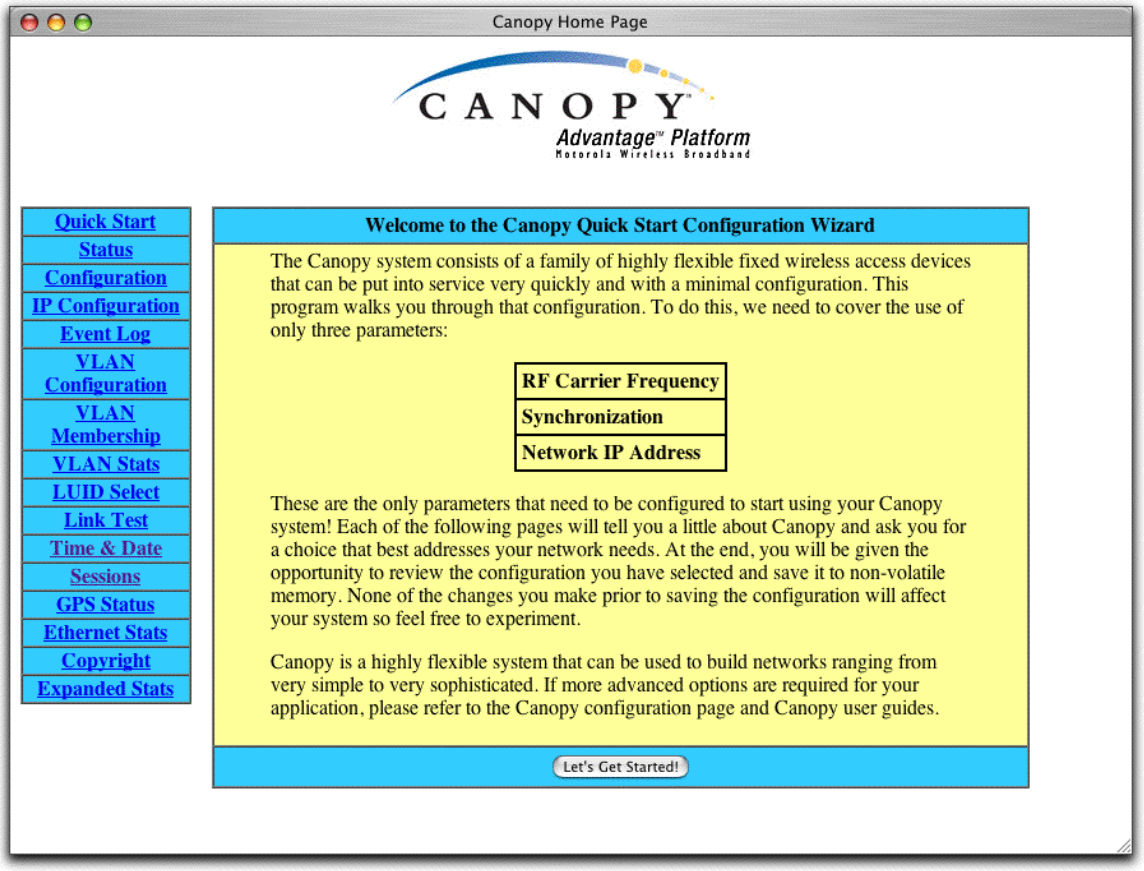

Canopy Home Page
CANOPY
Advantage™ Platform
Motorola Wireless Broadband
Quick Start
Status
Configuration
IP Configuration
Event Log
VLAN Configuration
VLAN Membership
VLAN Stats
LUID Select
Link Test
Time & Date
Sessions
GPS Status
Ethernet Stats
Copyright
Expanded Stats
Welcome to the Canopy Quick Start Configuration Wizard
The Canopy system consists of a family of highly flexible fixed wireless access devices that can be put into service very quickly and with a minimal configuration. This program walks you through that configuration. To do this, we need to cover the use of only three parameters:
RF Carrier Frequency
Synchronization
Network IP Address
These are the only parameters that need to be configured to start using your Canopy system! Each of the following pages will tell you a little about Canopy and ask you for a choice that best addresses your network needs. At the end, you will be given the opportunity to review the configuration you have selected and save it to non-volatile memory. None of the changes you make prior to saving the configuration will affect your system so feel free to experiment.
Canopy is a highly flexible system that can be used to build networks ranging from very simple to very sophisticated. If more advanced options are required for your application, please refer to the Canopy configuration page and Canopy user guides.
Let's Get Started!

Figure 50: Quick Start screen, AP

Quick Start is a wizard that helps you to perform a basic configuration that places an AP into service. Only the following parameters must be configured:

- **RF Carrier Frequency**
- **Synchronization**
- **Network IP Address**

In each page under Quick Start, you can

- specify the settings to satisfy the requirements of the network.
- review the configuration selected.
- save the configuration to non-volatile memory.

Proceed with the test setup as follows.

Procedure 7: Using Quick Start to configure the AP for test

1. At the bottom of the Quick Start page, click the **Let's Get Started!** button.
   RESULT: The AP responds by opening the RF Carrier Frequency page.
2. From the pull-down menu in the lower left corner of this page, select a frequency for the test.
3. Click the **Go To Next Page =>** button.
   RESULT: The AP responds by opening the Synchronization page.
4. At the bottom of this page, select **Generate Sync Signal**.
5. Click the **Go To Next Page =>** button.
   RESULT: The AP responds by opening the Lan IP Address page.
6. At the bottom of this page, specify
   f. a **Lan IP Address**.
   g. a **Lan Subnet Mask**.
   h. a **Default Gateway**.
7. Click the **Go To Next Page =>** button.
   RESULT: The AP responds by opening the Review and Save Configuration page.
8. Ensure that the initial parameters for the AP are set as you intended.
9. Click the **Save Changes** button.
10. Click the **Reboot** button.
    RESULT: The AP responds with the message **Reboot Has Been Initiated…**
11. Trigger your browser to refresh the page until the AP redisplays the Status page.

========== **end of procedure** ==========

Canopy encourages you to experiment with the interface. Unless you save a configuration and reboot the AP after you save the configuration, none of the changes are effected.

16.3.2 Time & Date Page of the AP

To proceed with the test setup, click the **Time & Date** button on the left side of the Quick Start page. The AP responds by opening the Time & Date page. An example of the AP Time & Date web page is displayed in Figure 51.

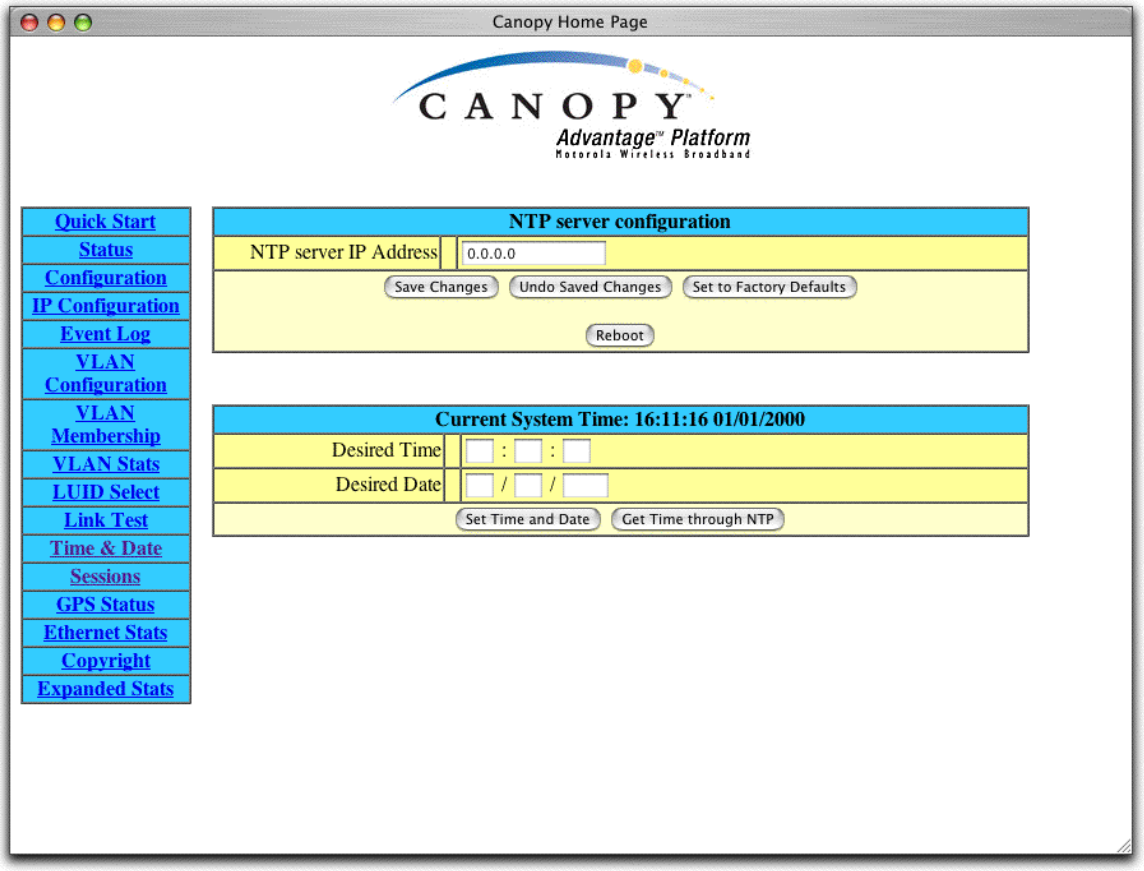


Figure 51: Time & Date screen, AP

To have each log in the AP correlated to a meaningful time and date, either a reliable network element must pass time and date to the AP or you must set the time and date whenever a power cycle of the AP has occurred. A network element passes time and date in any of the following scenarios:

- A connected CMM2 passes time and date (GPS time and date, if received).
- A connected CMMmicro passes the time and date (GPS time and date, if received), but only if both
  - the CMMmicro is operating on CMMmicro Release 2.1 or later release. (These releases include an NTP server functionality.)
  - the AP is operating on Canopy System Release 4.2 or later release. (These releases include an NTP client functionality.)
- A separate NTP server is addressable from the AP, and the AP is operating on Canopy System Release 4.2 or later release.

If the AP should derive time and date from either a CMMmicro or a separate NTP server, enter the IP address of the CMMmicro or NTP server on this web page. To force the AP to derive time and date before the first (or next) 15-minute interval query of the NTP server, click **Get Time through NTP**.

The format for entry is

Time ***hh:mm:ss***

Date ***mm/dd/yyyy***

where

hh represents the two-digit hour in the range 00 to 24

mm represents the two-digit minute

ss represents the two-digit second

mm represents the two-digit month

dd represents the two-digit day

yyyy represents the four-digit year

Proceed with the test setup as follows.

Procedure 8: Setting up the SM for test

1. Enter the appropriate information in the format shown above.
2. Click the **Set Time and Date** button.
   NOTE: The time displayed at the top of this page is static unless your browser is set to automatically refresh.
3. In one hand, securely hold the top (larger shell) of the SM. With the other hand, depress the lever in the back of the base cover (smaller shell). Remove the base cover.
4. Plug one end of a CAT 5 Ethernet cable into the SM.
5. Plug the other end of the Ethernet cable into the jack in the pig tail that hangs from the power supply.
6. Roughly aim the SM toward the AP.

WARNING!
From this point until you remove power from the SM, stay at least as far from the SM as the minimum separation distance specified under Preventing Overexposure to RF on Page 127.

7. Plug the power supply into an electrical outlet.
8. Repeat the foregoing steps for each SM that you wish to include in the test.
9. Back at the computing device, on the left side of the AP Time & Date page, click the **Sessions** button.
   RESULT: The AP responds by opening the Sessions page.

========== **end of procedure** ==========

16.3.3 Sessions Page of the AP

An example of the AP Sessions page is displayed in Figure 52.

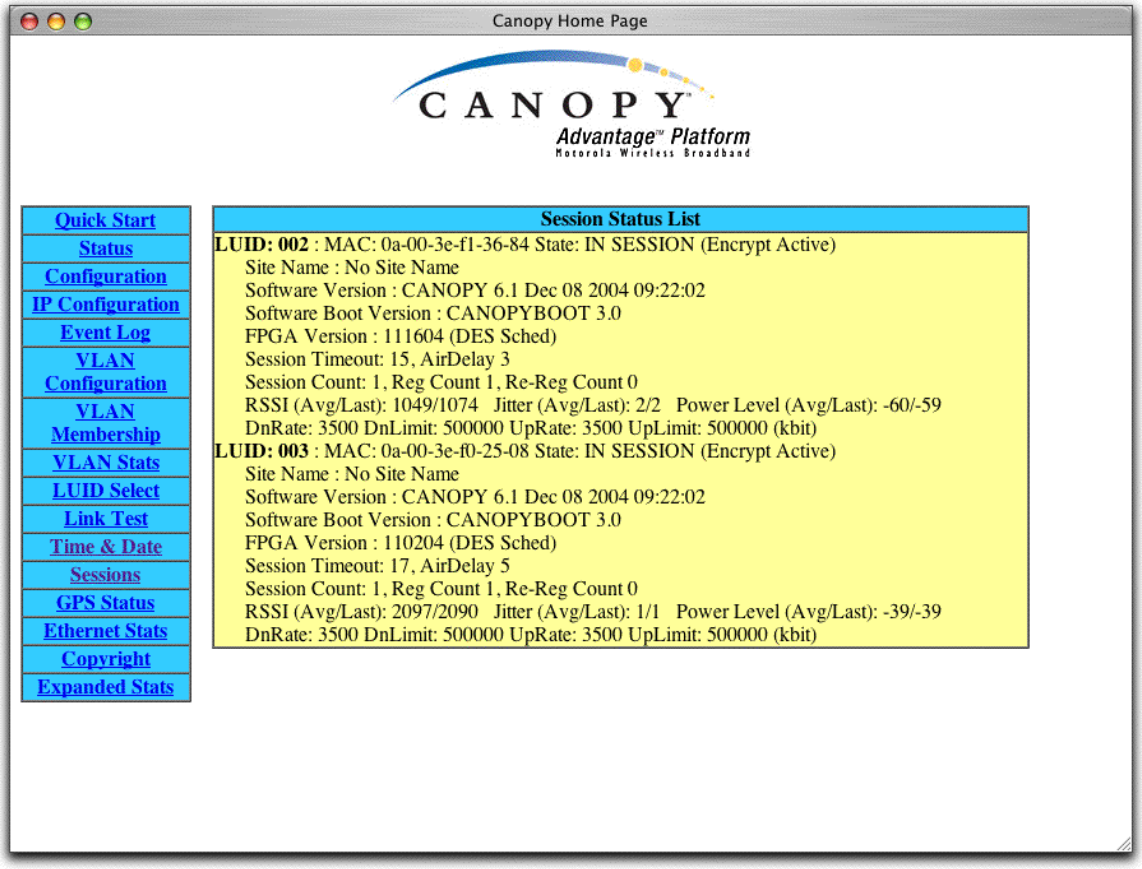

Canopy Home Page
CANOPY
Advantage™ Platform
Motorola Wireless Broadband
Quick Start
Status
Configuration
IP Configuration
Event Log
VLAN Configuration
VLAN Membership
VLAN Stats
LUID Select
Link Test
Time & Date
Sessions
GPS Status
Ethernet Stats
Copyright
Expanded Stats
Session Status List
LUID: 002 : MAC: 0a-00-3e-f1-36-84 State: IN SESSION (Encrypt Active)
Site Name : No Site Name
Software Version : CANOPY 6.1 Dec 08 2004 09:22:02
Software Boot Version : CANOPYBOOT 3.0
FPGA Version : 111604 (DES Sched)
Session Timeout: 15, AirDelay 3
Session Count: 1, Reg Count 1, Re-Reg Count 0
RSSI (Avg/Last): 1049/1074 Jitter (Avg/Last): 2/2 Power Level (Avg/Last): -60/-59
DnRate: 3500 DnLimit: 500000 UpRate: 3500 UpLimit: 500000 (kbit)
LUID: 003 : MAC: 0a-00-3e-f0-25-08 State: IN SESSION (Encrypt Active)
Site Name : No Site Name
Software Version : CANOPY 6.1 Dec 08 2004 09:22:02
Software Boot Version : CANOPYBOOT 3.0
FPGA Version : 110204 (DES Sched)
Session Timeout: 17, AirDelay 5
Session Count: 1, Reg Count 1, Re-Reg Count 0
RSSI (Avg/Last): 2097/2090 Jitter (Avg/Last): 1/1 Power Level (Avg/Last): -39/-39
DnRate: 3500 DnLimit: 500000 UpRate: 3500 UpLimit: 500000 (kbit)

Figure 52: Example Sessions page data, AP

If no SMs are registered to this AP, then the Sessions page displays the simple message **No sessions**. In this case, try the following steps.

Procedure 9: Retrying to establish a point-to-multipoint link

1. More finely aim the SM or SMs toward the AP.
2. Recheck the Sessions page of the AP for the presence of LUIDs.
3. If still no LUIDs are reported on the Sessions page, click the **Configuration** button on the left side of the page.
   RESULT: The AP responds by opening the AP Configuration page.
4. Scroll down to the **Color Code** parameter and note the setting.
5. In the same sequence as you did for the AP directly under Configuring a Point-to-Multipoint Link for Test on Page 138, connect the SM to a computing device and to power.
   RESULT: The SM powers up in the Operational mode, opens the SM Status page, scans, and attempts to register.

6. On the left side of the SM Status page, click the **Configuration** button. The Configuration page of the SM opens.
7. If the transmit frequency of the AP is not selected in the **Custom RF Frequency Scan Selection List** parameter, select the frequency that matches.
8. If the **Color Code** parameter on this page is not identical to the **Color Code** parameter you noted from the AP, change one of them so that they match.
9. At the bottom of the SM Configuration page, click **Save Changes**.
10. Click **Reboot**.
11. Allow several minutes for the SM to reboot and register to the AP.
12. Return to the computing device that is connected to the AP.
13. Recheck the Sessions page of the AP for the presence of LUIDs.

========== **end of procedure** ==========

The Sessions web page provides information about each SM that has registered to the AP. This information is useful for managing and troubleshooting a Canopy system. In Release 4.2 and later releases, all information that you have entered in the **Site Name** field of the SM displays in the Sessions page of the linked AP.

The Sessions page provides the following parameters.

LUID

This field displays the LUID (logical unit ID) of the SM. As each SM registers to the AP, the system assigns an LUID of 2 or a higher number to the SM. If an SM loses registration with the AP and then regains registration, the SM will retain the same LUID.

NOTE:
The LUID association is lost when a power cycle of the AP occurs.

MAC

This field displays the MAC address (or electronic serial number) of the SM.

State

This field displays the current status of the SM as either

- **IN SESSION** to indicate that the SM is currently registered to the AP.
- **IDLE** to indicate that the SM was registered to the AP at one time, but now is not.

Software Version

This field displays the software release that operates on the SM, the release date of the software, the time, and whether the module is secured by DES or AES encryption (see Encrypting Canopy Radio Transmissions on Page 296). When you request technical support, provide the information from this field.

An unpopulated **Software Version** parameter indicates a version earlier than Version 3.1.

Software Boot Version

This field indicates the CANOPYBOOT version number.

FPGA Version

This field displays the version of FPGA that runs on the SM. An unpopulated **FPGA Version** parameter indicates that a version earlier than Version 082002 runs on the SM.

Session Timeout

This field indicates the maximum interval in hours that the SM may sustain a single session with this AP.

AirDelay

This field displays the distance of the SM from the AP. To derive the distance in meters, multiply the displayed number by 0.3048. To derive the distance in feet, multiply the displayed number by 49. However, at close distances, the value in this field is unreliable. For example, at a distance of 12 feet, the **AirDelay** field may display a value of 7 (343 feet).

Session Count

This field displays how many sessions the SM has had with the AP. If the number of sessions is far greater than the number that other SMs registered to the AP have had, then this SM may have an installation problem.

Reg Count

This field displays how many registration request messages the AP has received from the SM. If the number of these messages is far greater than the number from other SMs registered to the AP, then this SM may have an installation problem.

Re-Reg Count

This field displays how many registration request messages the AP has received from the SM that is already in session. If the number of these messages is far greater than the number from other SMs that are both registered to the AP and in session, then this SM may have an installation problem.

RSSI (Avg/Last)

This field displays the average and the latest RSSI (received signal strength indicator) value for the SM.

Jitter (Avg/Last)

This field displays the average and the latest jitter value for the SM.

Power Level (Avg/Last)

This field displays the average and the latest power level set for the SM.

To begin the test

1. Note the LUID associated with the MAC address of any SM you wish to involve in the test.
2. On the left side of the Sessions page, click the **LUID Select** button.
   RESULT: The AP responds by opening the LUID Select page.

16.3.4 LUID Select Page of the AP

An example of an AP LUID Select screen is displayed in Figure 53.

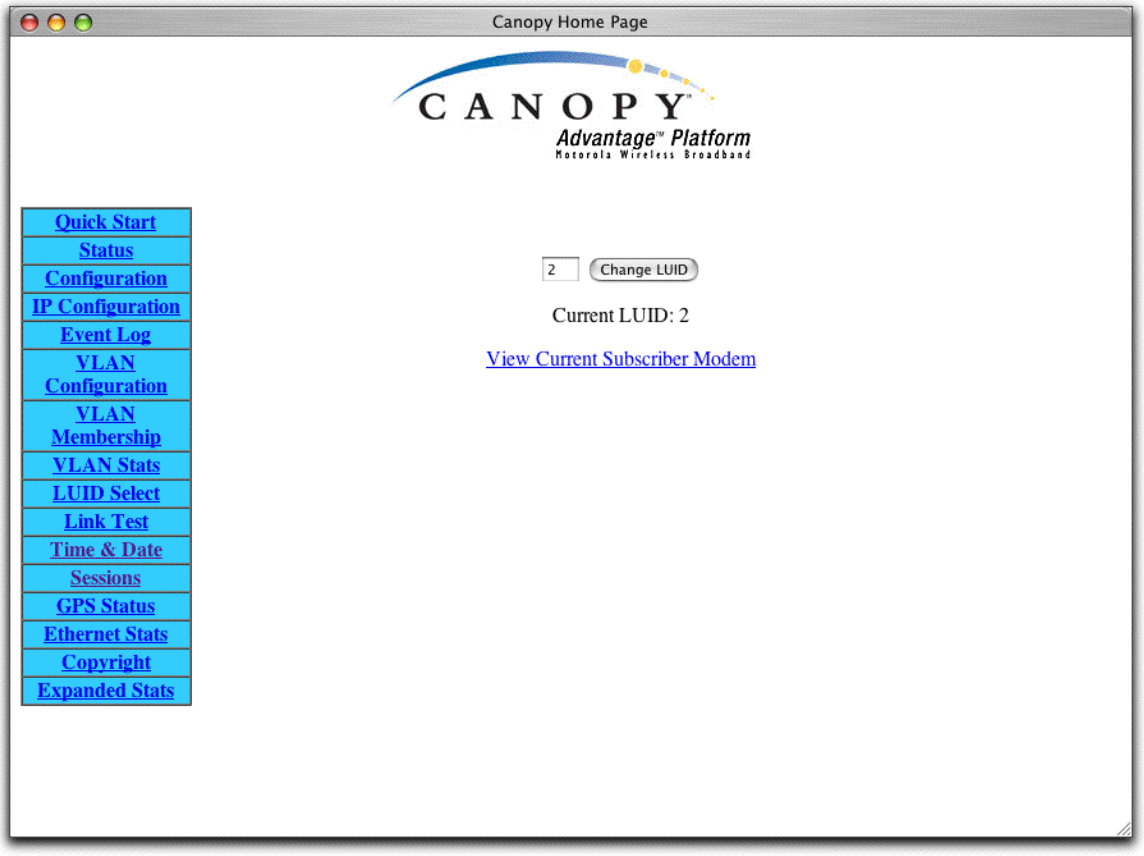


Figure 53: LUID Select screen, AP

This web page allows you to view the web pages of registered SMs over the RF link.

To view the pages for a selected SM, perform the following steps.

Procedure 10: Viewing SM pages through the AP

1. If the LUID differs from the LUID shown on the **Current LUID** line, enter the LUID into the **Change LUID** field.
2. Click the **Change LUID** button so that the LUID you entered in the previous step is shown on the **Current LUID** line.
3. Click **View Current Subscriber Modem**.
   RESULT: The Status page of the SM is displayed.

========== **end of procedure** ==========

16.3.5 Status Page of the SM

Examples of SM Status screens are displayed in Figure 54.

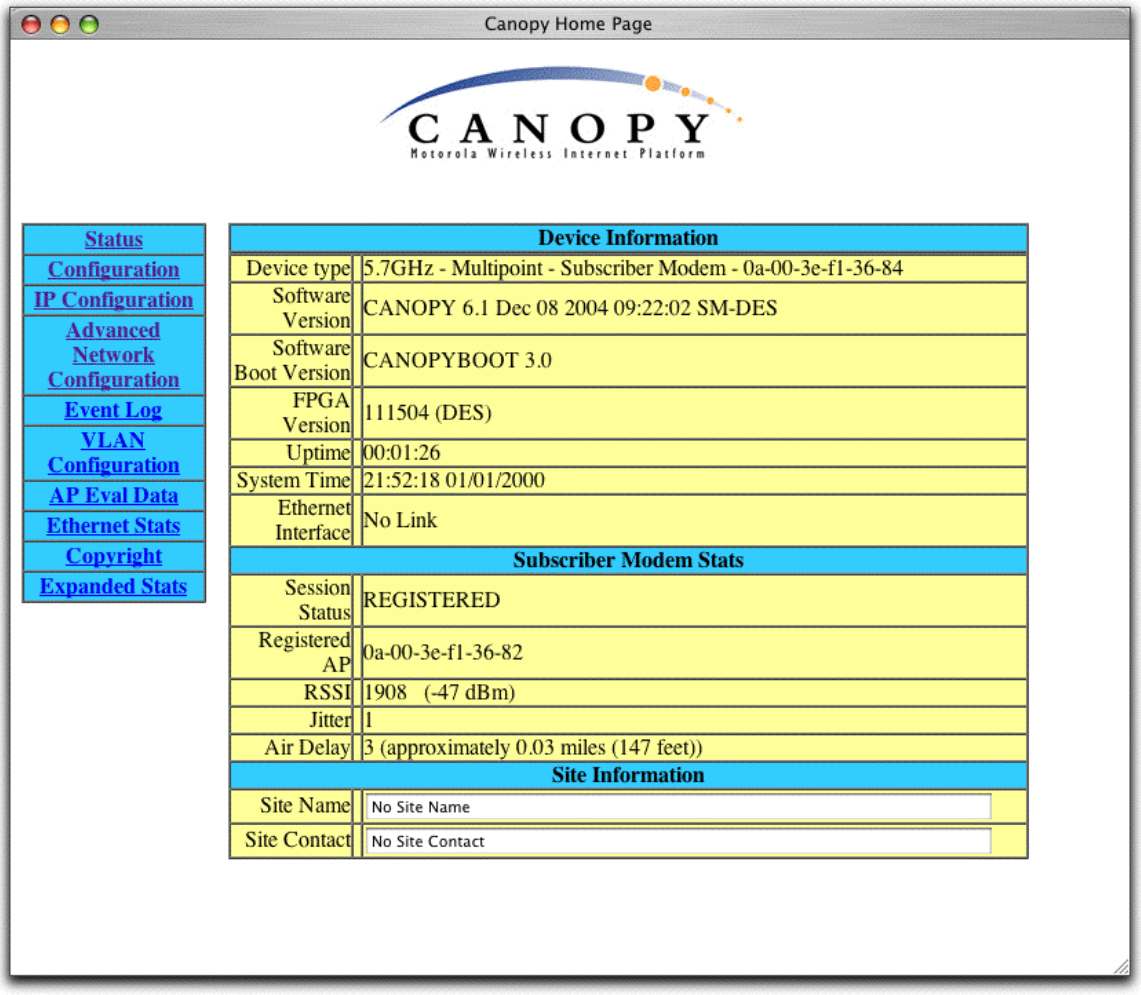


Figure 54: Status screen, SM

The Status page provides information on the operation of this SM. This is the default web page for the SM. The Status page provides the following fields.

Device Type

This field indicates the type of the Canopy module. Values include the frequency band of the module, the protocol that is used, and the MAC address of the module.

Canopy Boot Version

This field indicates the version of the software that is operated on the module, the date and time of boot, and whether the module is secured by DES or AES encryption (see Encrypting Canopy Radio Transmissions on Page 296). When you request technical support, provide the information from this field.

FPGA Version

This field indicates the version of the field-programmable gate array (FPGA) on the module. When you request technical support, provide the information from this field.

Uptime

This field indicates how long the module has operated since power was applied.

System Time

This field provides the current time. Any SM that registers to an AP inherits the system time, which is displayed in this field as GMT (Greenwich Mean Time).

Ethernet Interface

This field indicates the configuration of the Ethernet interface on the module.

Session Status

This field displays the following information about the current session:

- **Scanning** indicates that this SM currently cycles through the RF frequencies that are selected in the Configuration page. (See Custom RF Frequency Scan Selection List on Page 208.
- **Syncing** indicates that this SM currently attempts to receive sync.
- **Registering** indicates that this SM has sent a registration request message to the AP and has not yet received a response.
- **Registered** indicates that this SM is both
  - registered to an AP.
  - ready to transmit and receive data packets.
- **Alignment** indicates that this SM is in an aiming mode. See
  - Table 36 on Page 133.
  - Figure 112 on Page 280.

Registered AP

This field displays the IP address of the AP to which this SM is registered.

RSSI

This field displays the current RSSI (Radio Signal Strength Indicator)

- for the signal from the AP to which the SM is registered if the SM is registered.
- from any beacon if the SM is scanning.

An acceptable link has an RSSI of greater than 700. However, to achieve the best link possible, the alignment of the module should balance good RSSI values against good jitter values.

NOTE:
Unless the page is set to auto-refresh, the value displayed is the RSSI value at the instant the Status page was called. To keep a current view of the RSSI, refresh the browser screen or set to auto-refresh.

Jitter

This field displays the current quality of reception

- for the signal from the AP to which the SM is registered if the SM is registered.
- from any beacon if the SM is scanning.

An acceptable link has a jitter value between 0 and 4 in Release 4.0 and later releases or between 5 and 9 in any earlier release. However, to achieve the best link possible, the alignment of the module should balance good jitter values against good RSSI values.

NOTE:
Unless the page is set to auto-refresh, the value displayed is the jitter value at the instant the Status page was called. To keep a current view of the jitter, refresh the browser screen or set to auto-refresh.

Air Delay

This field displays the distance in feet between this SM and the AP. To derive the distance in meters, multiply the value of this parameter by 0.3048. Distances reported as less than 200 feet (61 meters) are unreliable.

Site Name

This field indicates the name of the physical module. You can assign or change this name on the Configuration web page. This information is also set into the *sysName* SNMP MIB-II object and can be polled by an SNMP management server.

Site Contact

This field indicates contact information for the physical module. You can provide or change this information on the Configuration web page. This information is also set into the *sysName* SNMP MIB-II object and can be polled by an SNMP management server.

To resume the test, perform the following steps.

Procedure 11: Verifying and recording information from SMs

1. Verify that the **Session Status** field of the SM Status page indicates **REGISTERED**.
   NOTE: This indication confirms that the SM is properly functional.
2. While your browser is set to this SM Status page, note (or print) the values of the following fields:
   - **Device type**
   - **Software Version**
   - **Software Boot Version**
   - **FPGA Version**
3. Systematically ensure that you can retrieve this data (from a database, for example) when you later prepare to deploy the SM to subscriber premises.
4. Return your browser to the Sessions page of the AP.
5. Note the LUID of the next SM that you wish to test.

6. Return your browser to the LUID Select page of the SM.
7. Repeat the test procedure from that point. When you have tested all of the SMs that you intend to test, return your browser to the Status page of the AP.

========== **end of procedure** ==========

16.3.6 Status Page of the AP

An example of an AP Status screen is displayed in Figure 55.

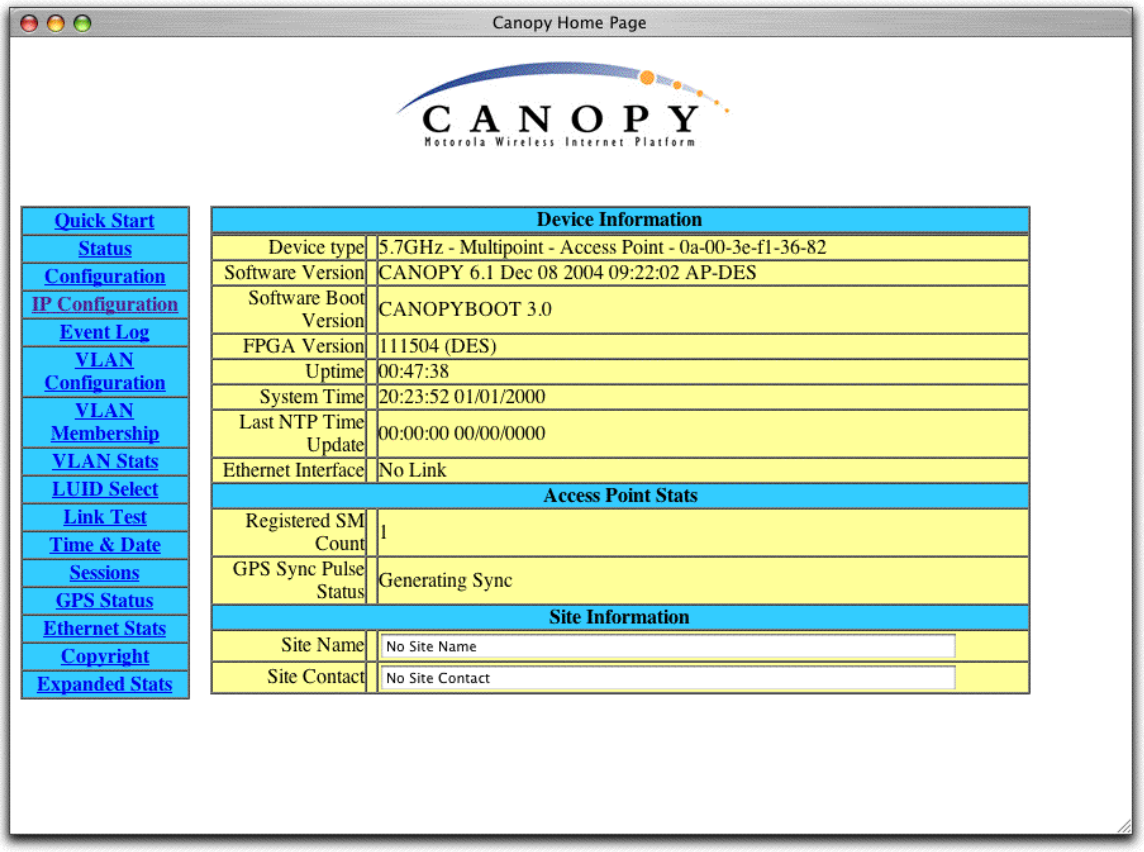


Figure 55: Status screen, AP

The Status page provides information on the operation of the module. This is the default web page for the module. The Status page provides the following fields.

Device Type

This field indicates the type of the Canopy module. Values include the frequency band of the module, the protocol that is used, and the MAC address of the module.

Software Version

This field indicates the software release that is operated on the module, the release date of the software, the time, and whether the module is secured by DES or AES encryption (see Encrypting Canopy Radio Transmissions on Page 296). When you request technical support, provide the information from this field.

Software Boot Version

This field indicates the CANOPYBOOT version number.

FPGA Version

This field indicates the version of the field-programmable gate array (FPGA) on the module. When you request technical support, provide the information from this field.

Uptime

This field indicates how long the module has operated since power was applied.

System Time

This field provides the current time. If the AP is connected to a CMM, then this field provides GMT (Greenwich Mean Time). Any SM that registers to the AP inherits the system time.

Ethernet Interface

This field indicates the configuration of the Ethernet interface on the module.

Registered SM Count

This field indicates how many SMs are registered to the AP.

GPS Sync Pulse Status

This field indicates the status of synchronization that the AP is receiving as follows:

- **Generating sync** indicates that the module is set to *generate* the sync pulse.
- **Receiving Sync** indicates that the module is set to *receive* a sync pulse from an outside source and is receiving the pulse.
- **ERROR: No Sync Pulse** indicates that the module is set to *receive* a sync pulse from an outside source and is not receiving the pulse.

NOTE:
When this message is displayed, the AP transmitter is turned off to avoid self-interference within the Canopy system.

Site Name

This field indicates the name of the physical module. You can assign or change this name on the Configuration web page. This information is also set into the *sysName* SNMP MIB-II object and can be polled by an SNMP management server.

Site Contact

This field indicates contact information for the physical module. You can provide or change this information on the Configuration web page. This information is also set into the *sysName* SNMP MIB-II object and can be polled by an SNMP management server.

To conclude the test, perform the following steps.

Procedure 12: Verifying and recording information from the AP

1. Confirm that the **GPS Sync Pulse Status** field indicates **Generating Sync**.
   NOTE: This indication confirms that the AP is properly functional.
2. While your browser is set to this AP Status page, note (or print) the values of the following fields:
   - **Device type**
   - **Software Version**
   - **Software Boot Version**
   - **FPGA Version**
3. Systematically ensure that you can retrieve this data when you prepare to deploy the AP.

========== **end of procedure** ==========

16.4 CONFIGURING A POINT-TO-POINT LINK FOR TEST

Perform the following steps to begin the test setup.

Procedure 13: Setting up the BH for Quick Start

1. In one hand, securely hold the top (larger shell) of the BH that you intend to deploy as a timing master. With the other hand, depress the lever in the back of the base cover (smaller shell). Remove the base cover.
2. Plug one end of a CAT 5 Ethernet cable into the timing master.
3. Plug the other end of the Ethernet cable into the jack in the pig tail that hangs from the power supply.
4. Plug the other connector of the pig tail into the Ethernet jack of the computing device.

WARNING!
From this point until you remove power from the BH, stay at least as far from the BH as the minimum separation distance specified under Preventing Overexposure to RF on Page 127.

5. Plug the power supply into an electrical outlet.
6. Power up the computing device.

7. Start the browser in the computing device.
8. Access the Configuration page of the BH.
9. In the **Timing Mode** parameter, select **Timing Master**.
10. Click **Save Changes**.
11. Click **Reboot**.

end of procedure

The Canopy BH interface provides a series of web pages to configure and monitor the unit. These screens are subject to change by subsequent software releases.

You can access the web-based interface through only a computing device that is either directly connected or connected through a network to the BH. If the computing device is not connected to a network when you are configuring the module in your test environment, and if the computer has used a proxy server address and port to configure a Canopy module, then you may need to first disable the proxy setting in the computer.

To toggle the computer to *not* use the proxy setting, perform Procedure 6 on Page 139.

In the address bar of your browser, enter the IP address of the BHM (default is 169.254.1.1). The BHM responds by opening the Status page.

16.4.1 Quick Start Page of the BHM

To proceed with the test setup, click the **Quick Start** button on the left side of the Status page. The BHM responds by opening the Quick Start page. The standard Quick Start screen is displayed in Figure 56.

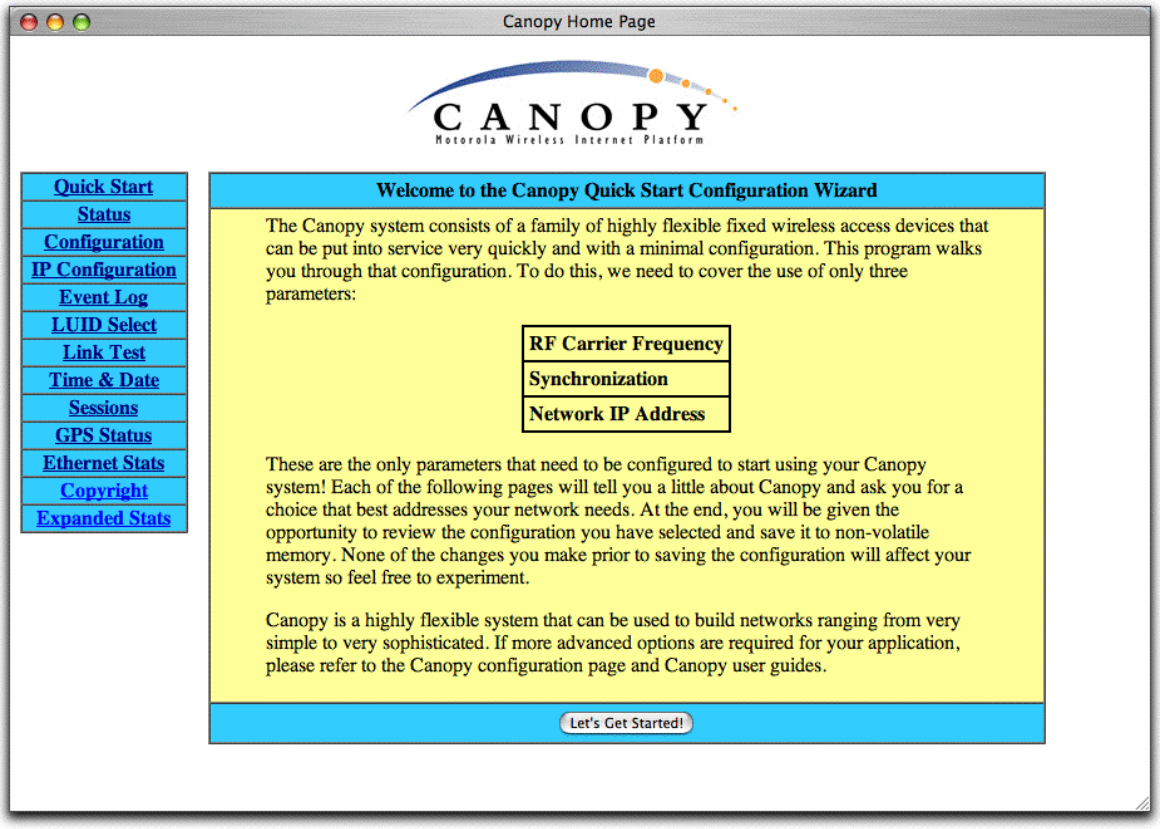

Canopy Home Page
CANOPY
Motorola Wireless Internet Platform
Quick Start
Status
Configuration
IP Configuration
Event Log
LUID Select
Link Test
Time & Date
Sessions
GPS Status
Ethernet Stats
Copyright
Expanded Stats
Welcome to the Canopy Quick Start Configuration Wizard
The Canopy system consists of a family of highly flexible fixed wireless access devices that can be put into service very quickly and with a minimal configuration. This program walks you through that configuration. To do this, we need to cover the use of only three parameters:
RF Carrier Frequency
Synchronization
Network IP Address
These are the only parameters that need to be configured to start using your Canopy system! Each of the following pages will tell you a little about Canopy and ask you for a choice that best addresses your network needs. At the end, you will be given the opportunity to review the configuration you have selected and save it to non-volatile memory. None of the changes you make prior to saving the configuration will affect your system so feel free to experiment.
Canopy is a highly flexible system that can be used to build networks ranging from very simple to very sophisticated. If more advanced options are required for your application, please refer to the Canopy configuration page and Canopy user guides.
Let's Get Started!

Figure 56: Quick Start screen, BHM

Quick Start is a wizard that helps you to perform a basic configuration that places a BHM into service. Only the following parameters must be configured:

- **RF Carrier Frequency**
- **Synchronization**
- **Network IP Address**

In each page under Quick Start, you can

- specify the settings to satisfy the requirements of the network.
- review the configuration selected.
- save the configuration to non-volatile memory.

Proceed with the test setup as follows.

Procedure 14: Using Quick Start to configure the BH for test

1. At the bottom of the Quick Start page, click the **Let's Get Started!** button.
   RESULT: The BHM responds by opening the RF Carrier Frequency page.
2. From the pull-down menu in the lower left corner of this page, select a frequency for the test.
3. Click the **Go To Next Page =>** button.
   RESULT: The BHM responds by opening the Synchronization page.

4. At the bottom of this page, select **Generate Sync Signal**.
5. Click the **Go To Next Page =>** button.
   RESULT: The BHM responds by opening the Lan IP Address page.
6. At the bottom of this page, specify
   a. a **Lan IP Address**.
   b. a **Lan Subnet Mask**.
   c. a **Default Gateway**.
7. Click the **Go To Next Page =>** button.
   RESULT: The BHM responds by opening the Review and Save Configuration page.
8. Ensure that the initial parameters for the BHM are set as you intended.
9. Click the **Save Changes** button.
10. On the left side of the Status page, click the **Configuration** button.
    RESULT: The BHM responds by opening the Configuration page.
11. In the **Timing Mode** parameter, select **Timing Master**.
    RESULT: This BH is now forced to provide sync for the link and the distinct set of web interface pages and parameters for the role of BHM.
12. Click the **Save Changes** button.
13. Click the **Reboot** button.
    RESULT: The BHM responds with the message **Reboot Has Been Initiated…**
14. Trigger your browser to refresh the page until the BHM redisplays the Status page.

end of procedure

We encourage you to experiment with the interface. Unless you save a configuration and reboot the BHM after you save the configuration, none of the changes are effected.

16.4.2 Time & Date Page of the BHM

To proceed with the test setup, click the **Time & Date** button on the left side of the Quick Start page. The BHM responds by opening the Time & Date page. An example of the BHM Time & Date web page is displayed in Figure 57.

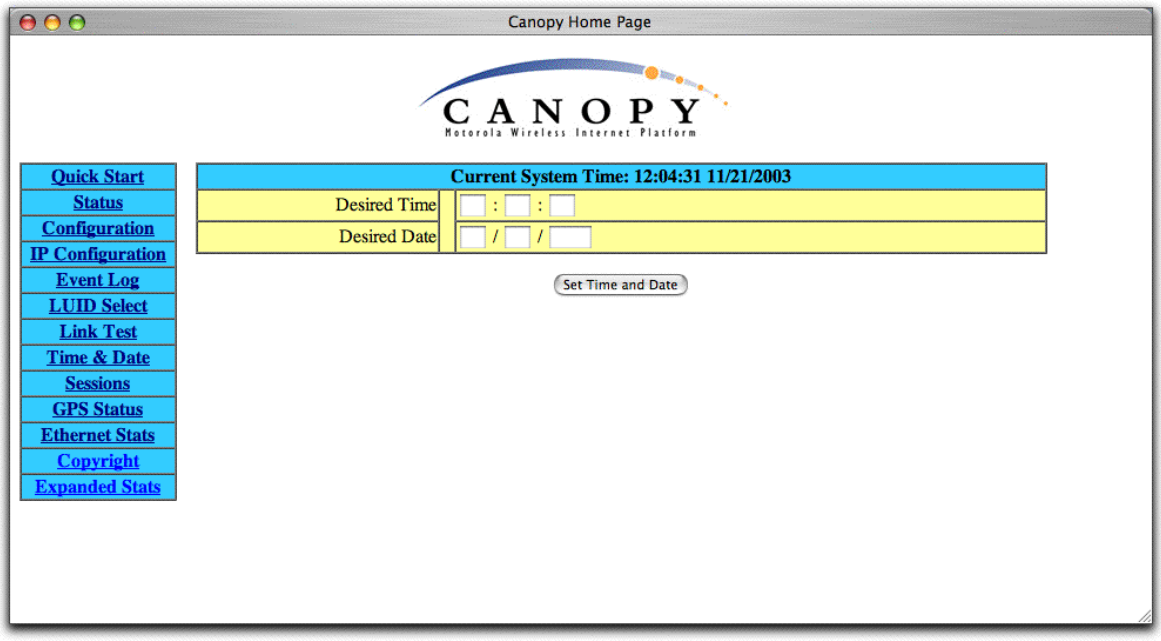


Figure 57: Time & Date screen, BHM

To have each log in the BHM correlated to a meaningful time and date, either a reliable network element must pass time and date to the BHM or you must set the time and date whenever a power cycle of the BHM has occurred. A network element passes time and date in any of the following scenarios:

- A connected CMM2 passes time and date (GPS time and date, if received).
- A connected CMMmicro passes the time and date (GPS time and date, if received), but only if both
  - the CMMmicro is operating on CMMmicro Release 2.1 or later release. (These releases include an NTP server functionality.)
  - the BHM is operating on Canopy System Release 4.2 or later release. (These releases include an NTP client functionality.)
- A separate NTP server is addressable from the BHM, and the BHM is operating on Canopy System Release 4.2 or later release.

If the BHM should derive time and date from either a CMMmicro or a separate NTP server, enter the IP address of the CMMmicro or NTP server on this web page. To force the BHM to derive time and date before the first (or next) 15-minute interval query of the NTP server, click **Get Time through NTP**.

If you must set the time and date, use the following format for entry:

Time ***hh:mm:ss***

Date ***mm/dd/yyyy***

where

hh	represents the two-digit hour in the range 00 to 24
mm	represents the two-digit minute
ss	represents the two-digit second
mm	represents the two-digit month
dd	represents the two-digit day
yyyy	represents the four-digit year

Proceed with the test setup as follows.

Procedure 15: Setting up the BHS for test

1. Enter the appropriate information in the format shown above.
2. Click the **Set Time and Date** button.
   NOTE: The time displayed at the top of this page is static unless your browser is set to automatically refresh.
3. In one hand, securely hold the top (larger shell) of the BH that you intend to deploy as a timing slave. With the other hand, depress the lever in the back of the base cover (smaller shell). Remove the base cover.
4. Plug one end of a CAT 5 Ethernet cable into the BHS.
5. Plug the other end of the Ethernet cable into the jack in the pig tail that hangs from the power supply.
6. Roughly aim the BHS toward the BHM.

WARNING!
From this point until you remove power from the BHS, stay at least as far from the BHS as the minimum separation distance specified under Preventing Overexposure to RF on Page 127.

7. Plug the power supply into an electrical outlet.
8. Back at the computing device, on the left side of the BHM Time & Date page, click the **Sessions** button.
   RESULT: The BHM responds by opening the Sessions page.

========== **end of procedure** ==========

16.4.3 Sessions Page of the BHM

An example of the BHM Sessions page is displayed in Figure 58.

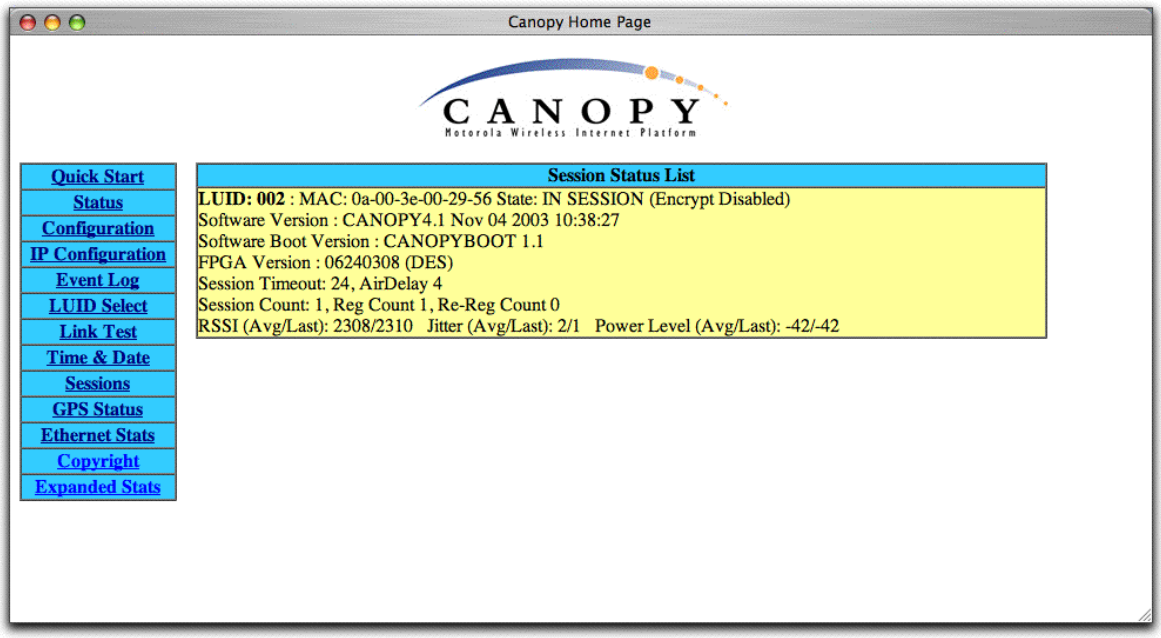


Figure 58: Example Sessions page data, BHM

If the BHS is not registered to this BHM, then the Sessions page displays the simple message **No sessions**. In this case, try the following steps.

Procedure 16: Retrying to establish a point-to-point link

1. More finely aim the BHS toward the BHM.
2. Recheck the Sessions page of the BHM for the presence of the BHS LUID.
3. If the LUID is still not reported on the Sessions page, click the **Configuration** button on the left side of the page.
   RESULT: The BHM responds by opening the BHM Configuration page.
4. Scroll down to the **Color Code** parameter and note the setting.
5. In the same sequence as you did for the BHM directly under Configuring a Point-to-Point Link for Test on Page 153, connect the BHS to a computing device and to power.
   RESULT: The BHS powers up in the Operational mode, opens the SM Status page, scans, and attempts to register.
6. On the left side of the BHS Status page, click the **Configuration** button. The Configuration page of the BHS opens.
7. In the **Timing Mode** parameter, select **Timing Slave**.
   RESULT: This BH is now forced to receive sync and to provide the distinct set of web interface pages and parameters for the role of BHS.

8. Click the **Save Changes** button.
9. Click the **Reboot** button.
   RESULT: The BHS responds with the message **Reboot Has Been Initiated…**
10. Trigger your browser to refresh the page until the BHS redisplays the Status page.
11. If the transmit frequency of the BHM is not selected in the **Custom RF Frequency Scan Selection List** parameter, select the frequency that matches.
12. If the **Color Code** parameter on this page is not identical to the **Color Code** parameter you noted from the BHM, change one of them so that they match.
13. At the bottom of the BHS Configuration page, click **Save Changes**.
14. Click **Reboot**.
15. Allow several minutes for the BHS to reboot and register to the BHM.
16. Return to the computing device that is connected to the BHM.
17. Recheck the Sessions page of the BHM for the presence of the BHS LUID.

end of procedure

The Sessions web page provides information about the BHS that has registered to the BHM. This information is useful for managing and troubleshooting a Canopy system. In Release 4.2 and later releases, all information that you have entered in the **Site Name** field of the BHS displays in the Sessions page of the linked BHM.

The Sessions page provides the following fields.

LUID

This field displays the LUID (logical unit ID) of the BHS. As the BHS registers to the BHM, the BHM assigns an LUID of 2 to the BHS. If the BHS loses registration with the BHM and then regains registration, the BHS will retain the same LUID.

NOTE:
The LUID association is lost when a power cycle of the BHM occurs.

MAC

This field displays the MAC address (or electronic serial number) of the BHS.

State

This field displays the current status of the BHS as either

- **IN SESSION** to indicate that the BHS is currently registered to the BHM.
- **IDLE** to indicate that the BHS was registered to the BHM at one time, but now is not.

Software Version

This field displays the software release that operates on the BHS, the release date of the software, the time, and whether the module is secured by DES or AES encryption (see Encrypting Canopy Radio Transmissions on Page 296). When you request technical support, provide the information from this field.

An unpopulated **Software Version** parameter indicates a version earlier than Version 3.1.

Software Boot Version

This field indicates the CANOPYBOOT version number.

FPGA Version

This field displays the version of field programmable gate array (FPGA) that runs on the BHS. An unpopulated **FPGA Version** parameter indicates a version earlier than Version 082002.

Session Timeout

This field indicates the maximum interval in hours that the BHS may sustain a single session with this BHM.

AirDelay

This field displays the distance of the BHS from the BHM. To derive the distance in meters, the multiply the displayed number by 0.3048. To derive the distance in feet, multiply the displayed number by 49. However, at close distances, the value in this field is unreliable. For example, at a distance of 12 feet, the **AirDelay** field may display a value of 7 (343 feet).

Session Count

This field displays how many sessions the BHS has had with the BHM. If the number of sessions is abnormally high, then this BHS may have an installation problem.

Reg Count

This field displays how many registration request messages the BHM has received from the BHS. If the number of these messages is abnormally high, then this BHS may have an installation problem.

Re-Reg Count

This field displays how many registration request messages the BHM has received from the BHS that is already in session. If the number of these messages is abnormally high, then this BHS may have an installation problem.

RSSI (Avg/Last)

This field displays the average and the latest RSSI (received signal strength indicator) value for the BHS.

Jitter (Avg/Last)

This field displays the average and the latest jitter value for the BHS.

Power Level (Avg/Last)

This field displays the average and the latest power level set for the BHS.

To begin the test, perform the following steps.

Procedure 17: Viewing BHS pages through the BHM

1. Note the LUID associated with the MAC address of the BHS.
2. On the left side of the Sessions page, click the **LUID Select** button.
   RESULT: The BHM responds by opening the LUID Select page.

========== **end of procedure** ==========

16.4.4 LUID Select Page of the BHM

An example of a BHM LUID Select screen is displayed in Figure 59.

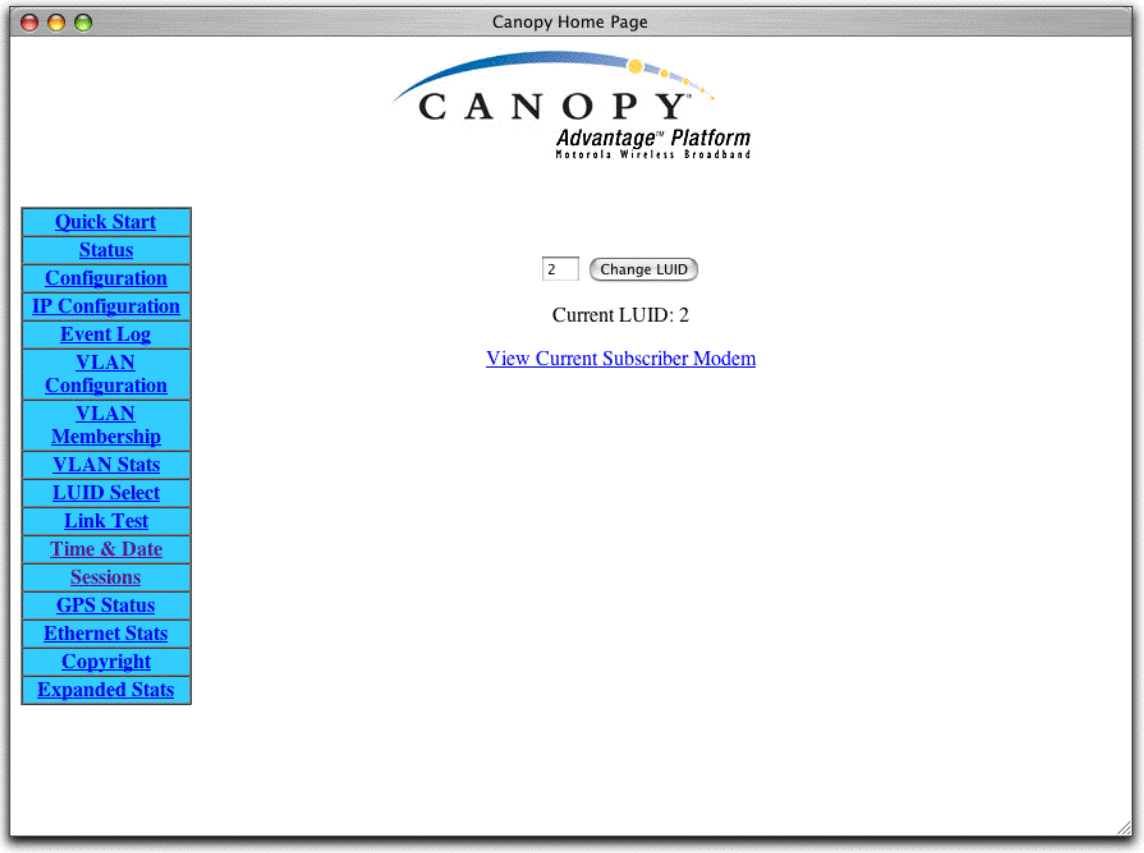


Figure 59: LUID Select screen, BHM

This web page allows you to view the web pages of a registered BHS over the RF link. To view the pages for the BHS, perform the following steps.

Procedure 18: Viewing BHS pages through the BHM

1. Verify that the LUID matches the LUID shown on the **Current LUID** line.
2. Click **View Current Subscriber Modem**.
   RESULT: The Status page of the BHS is displayed.

========== **end of procedure** ==========

16.4.5 Status Page of the BHS

An example of the BHS Status screen is displayed in Figure 60.

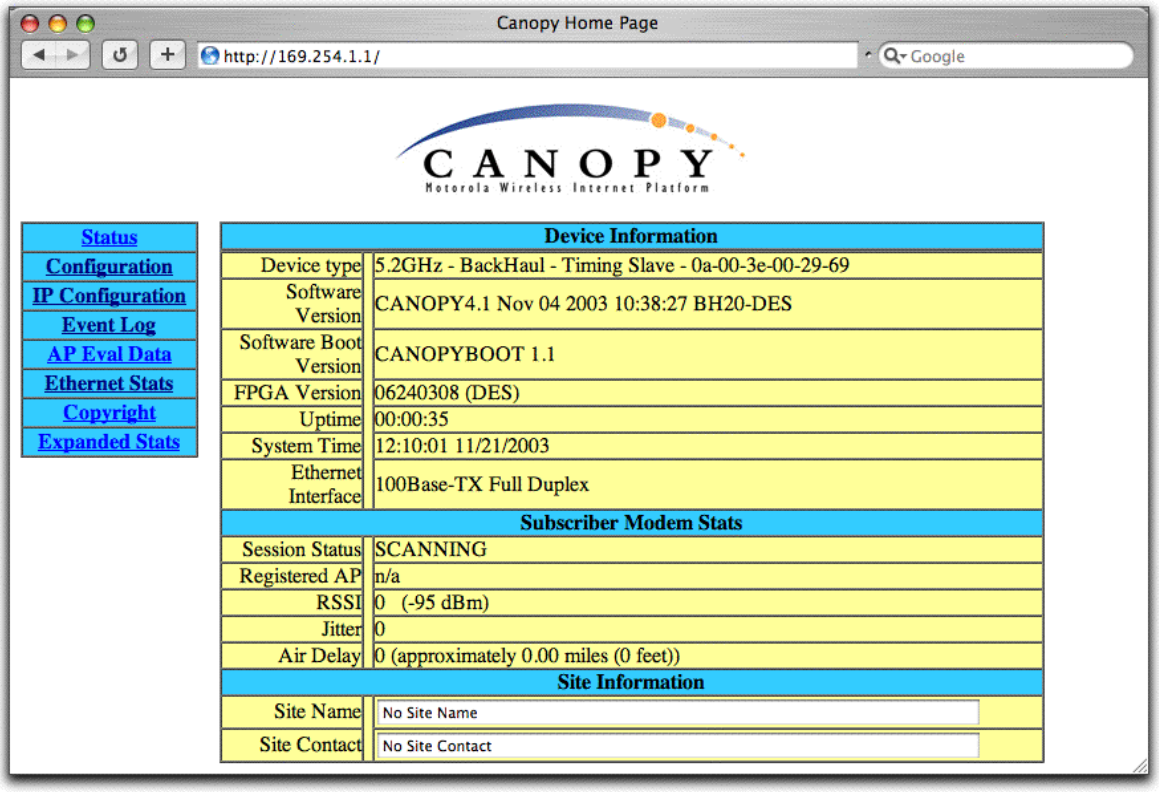


Figure 60: Status screen, 5.2-GHz BHS

The Status page provides information on the operation of this BHS. This is the default web page for the BHS. The Status page provides the following parameters.

Device Type

This field indicates the type of the Canopy module. Values include the frequency band of the module, the protocol that is used, and the MAC address of the module.

Canopy Boot Version

This field indicates the version of the software that is operated on the module, the date and time of boot, and whether the module is secured by DES or AES encryption (see Encrypting Canopy Radio Transmissions on Page 296). When you request technical support, provide the information from this field.

FPGA Version

This field indicates the version of the field-programmable gate array (FPGA) on the module. When you request technical support, provide the information from this field.

Uptime

This field indicates how long the module has operated since power was applied.

System Time

This field provides the current time. The BHS that registers to the BHM inherits the system time, which is displayed in this field as GMT (Greenwich Mean Time).

Ethernet Interface

This field indicates the configuration of the Ethernet interface on the module.

Session Status

This field displays the following information about the current session:

- **Scanning** indicates that this BHS currently cycles through the RF frequencies that are selected in the Configuration page. (See Custom RF Frequency Scan Selection List on Page 208.
- **Syncing** indicates that this BHS currently attempts to receive sync.
- **Registering** indicates that this BHS has sent a registration request message to the BHM and has not yet received a response.
- **Registered** indicates that this BHS is both
  - registered to a BHM.
  - ready to transmit and receive data packets.
- **Alignment** indicates that this BHS is in an aiming mode. See
  - Table 36 on Page 133.
  - Figure 112 on Page 280.

Registered AP

This field displays the IP address of the BHM to which this BHS is registered.

RSSI

This field displays the current RSSI (Radio Signal Strength Indicator)

- for the signal from the BHM if the BHS is registered.
- from any beacon if the SM is scanning.

An acceptable link has an RSSI of greater than 700. However, to achieve the best link possible, the alignment of the module should balance good RSSI values against good jitter values.

NOTE:
Unless the page is set to auto-refresh, the value displayed is the RSSI value at the instant the Status page was called. To keep a current view of the RSSI, refresh the browser screen or set to auto-refresh.

Jitter

This field displays the current quality of reception

- for the signal from the BHM if the BHS is registered.
- from any beacon if the BHS is scanning.

An acceptable link has a jitter value between 0 and 4 in Release 4.0 and later releases or between 5 and 9 in any earlier release. However, to achieve the best link possible, the alignment of the module should balance good jitter values against good RSSI values.

NOTE:
Unless the page is set to auto-refresh, the value displayed is the jitter value at the instant the Status page was called. To keep a current view of the jitter, refresh the browser screen or set to auto-refresh.

Air Delay

This field displays the distance in feet between this BHS and the BHM. To derive the distance in meters, the multiply the value of this parameter by 0.3048. Distances reported as less than 200 feet (61 meters) are unreliable.

Site Name

This field indicates the name of the physical module. You can assign or change this name on the Configuration web page. This information is also set into the *sysName* SNMP MIB-II object and can be polled by an SNMP management server.

Site Contact

This field indicates contact information for the physical module. You can provide or change this information on the Configuration web page. This information is also set into the *sysName* SNMP MIB-II object and can be polled by an SNMP management server.

To resume the test, perform the following steps.

Procedure 19: Verifying and recording information from the BHS

1. Verify that the **Session Status** field of the BHS Status page indicates **REGISTERED**.
   NOTE: This indication confirms that the BHS is properly functional.
2. While your browser is set to this BHS Status page, note (or print) the values of the following fields:
   - **Device type**
   - **Software Version**
   - **Software Boot Version**
   - **FPGA Version**
3. Systematically ensure that you can retrieve this data when you prepare to deploy the BHS.
4. Return your browser to the Status page of the BHM.

========== **end of procedure** ==========

16.4.6 Status Page of the BHM

An example of an BHM Status screen is displayed in Figure 61.

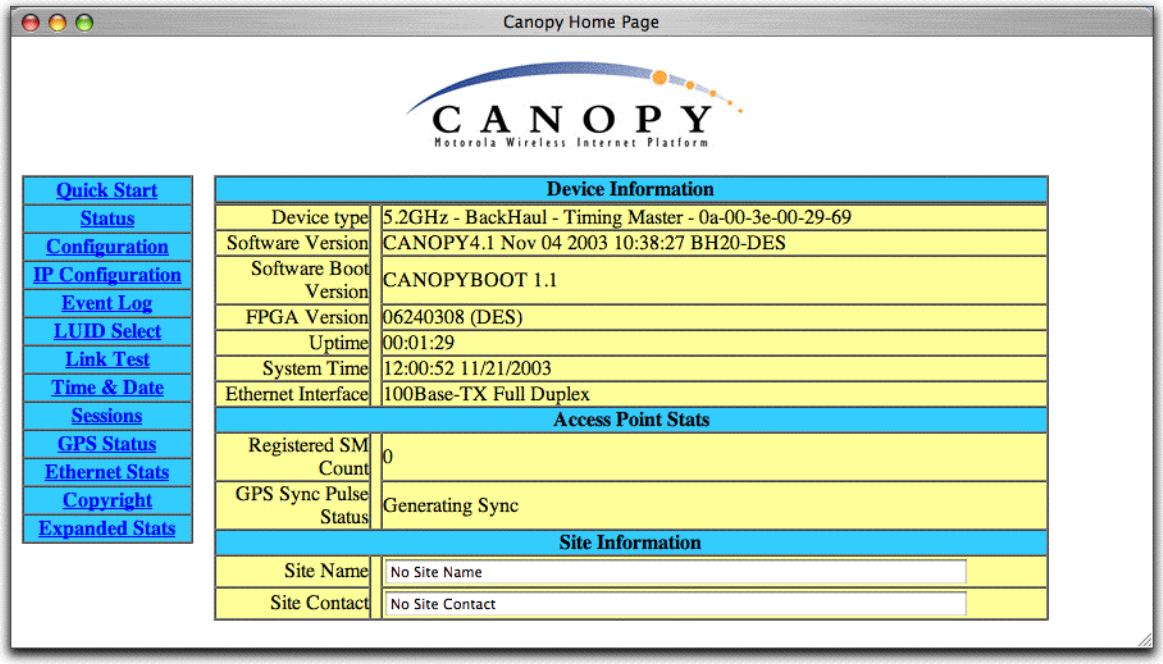


Figure 61: Status screen, BHM

The Status page provides information on the operation of the module. This is the default web page for the module. The Status page provides the following fields.

Device Type

This field indicates the type of the Canopy module. Values include the frequency band of the module, the protocol that is used, and the MAC address of the module.

Software Version

This field indicates the software release that is operated on the module, the release date of the software, the time, and whether the module is secured by DES or AES encryption (see Encrypting Canopy Radio Transmissions on Page 296). When you request technical support, provide the information from this field.

Software Boot Version

This field indicates the CANOPYBOOT version number.

FPGA Version

This field indicates the version of the field-programmable gate array (FPGA) on the module. When you request technical support, provide the information from this field.

Uptime

This field indicates how long the module has operated since power was applied.

System Time

This field provides the current time. If the BHM is connected to a CMM, then this field provides GMT (Greenwich Mean Time). The BHS that registers to the BHM inherits the system time.

Ethernet Interface

This field indicates the configuration of the Ethernet interface on the module.

Registered SM Count

This field indicates how many BHSs are registered to the BHM.

GPS Sync Pulse Status

This field indicates the status of synchronization that the BHM is receiving as follows:

- **Generating sync** indicates that the module is set to *generate* the sync pulse.
- **Receiving Sync** indicates that the module is set to *receive* a sync pulse from an outside source and is receiving the pulse.
- **ERROR: No Sync Pulse** indicates that the module is set to *receive* a sync pulse from an outside source and is not receiving the pulse.

NOTE:
When this message is displayed, the BHM transmitter is turned off to avoid self-interference within the Canopy system.

Site Name

This field indicates the name of the physical module. You can assign or change this name on the Configuration web page. This information is also set into the *sysName* SNMP MIB-II object and can be polled by an SNMP management server.

Site Contact

This field indicates contact information for the physical module. You can provide or change this information on the Configuration web page. This information is also set into the *sysName* SNMP MIB-II object and can be polled by an SNMP management server.

To conclude the test, perform the following steps.

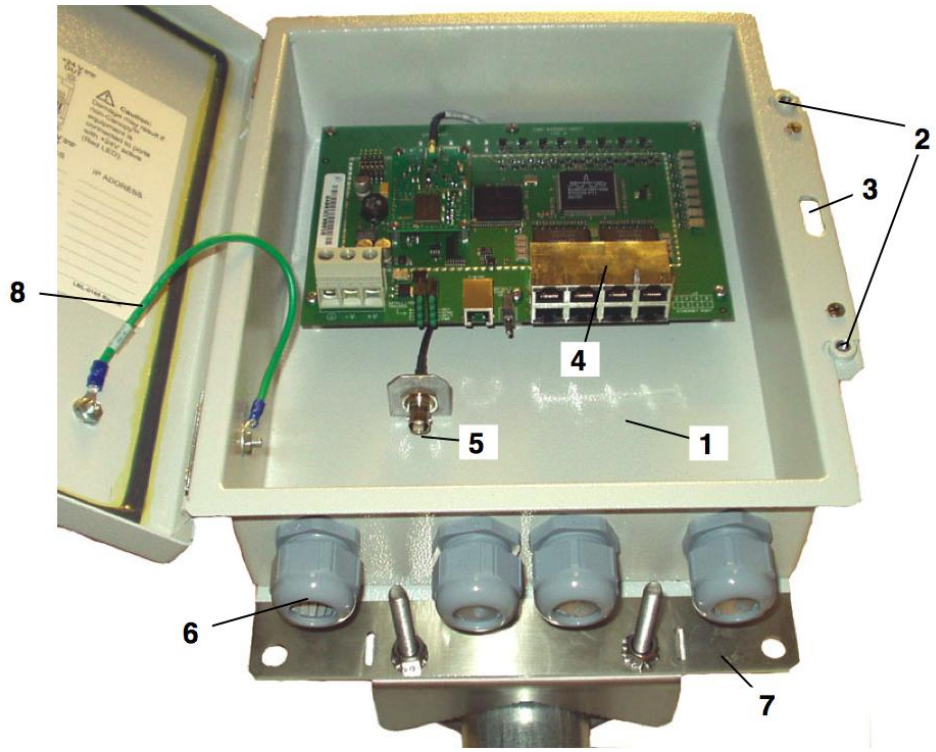
Procedure 20: Verifying and recording information from the BHM

1. Confirm that the **GPS Sync Pulse Status** field indicates **Generating Sync**.
   NOTE: This indication confirms that the BHM is properly functional.
2. While your browser is set to this BHM Status page, note (or print) the values of the following fields:
   - **Device type**
   - **Software Version**
   - **Software Boot Version**
   - **FPGA Version**
3. Systematically ensure that you can retrieve this data when you prepare to deploy the BHM.

end of procedure

16.4.7 Configuring a CMMmicro for Test

The layout of the CMMmicro is as shown in Figure 62.



1 **Weatherized enclosure**
2 **Thumb-screw/slot-screwdriver door fasteners**
3 **Punch-out for padlock**
4 **Ethernet switch and power module**
5 **Female BNC connector**
6 **Water-tight bulkhead connectors**
7 **Flange for attachment (stainless steel so it grounds to tower or building) using U bolts (provided) or other hardware such as screws or lag bolts or attachment straps (not provided).**
8 **Ground strap to ground door to enclosure**

Figure 62: CMMmicro layout

Perform the following procedure to configure the CMMmicro for testing.

IMPORTANT!
Start with the 24-V DC power converter *unconnected* to AC.

Procedure 21: Configuring a CMMmicro

1. Connect the converter lead whose insulation has a white stripe to +V on the CMMmicro terminal block.
2. Connect the converter lead whose insulation is solid black to -V on the CMMmicro terminal block.
3. Connect the power converter to an AC receptacle using the AC power cord.
4. Wait until the green LED labeled RDY flashes.
   NOTE: This should occur in less than one minute and will indicate that the CMMmicro has transitioned from booting to normal operation.
5. Observe which, if any, Ethernet ports are powered, as indicated by a lit red LED to the right of the Ethernet port.
   NOTE: The position of this +24-V OUT LED is shown in Figure 63 on Page 171.

CAUTION!
Never connect any devices other than Canopy APs and BHs to a powered port. Powered ports are indicated by a red LED to the right of the port. (See Item 7 in Figure 64 on Page 172.) A powered port has 24-V DC on Pins 7 and 8 and 24-V return on Pins 4 and 5. This can damage other networking equipment, such as a computer or a router.

6. On the 8-port Ethernet block of the CMMmicro, use either a straight-through or crossover Ethernet cable to connect any *unpowered* port (*without* the red LED lit) to a browser-equipped computer.
   NOTE: The CMMmicro auto-senses the cable type.
7. Verify these CMMmicro connections against Figure 65 on Page 173.
8. Configure the computer to use DHCP, with no proxy in your network settings.
9. Open the browser.
10. In the address bar, enter 169.254.1.1 (the default IP address of the CMMmicro).
    RESULT: The browser displays the CMMmicro Status page.

========== **end of procedure** ==========

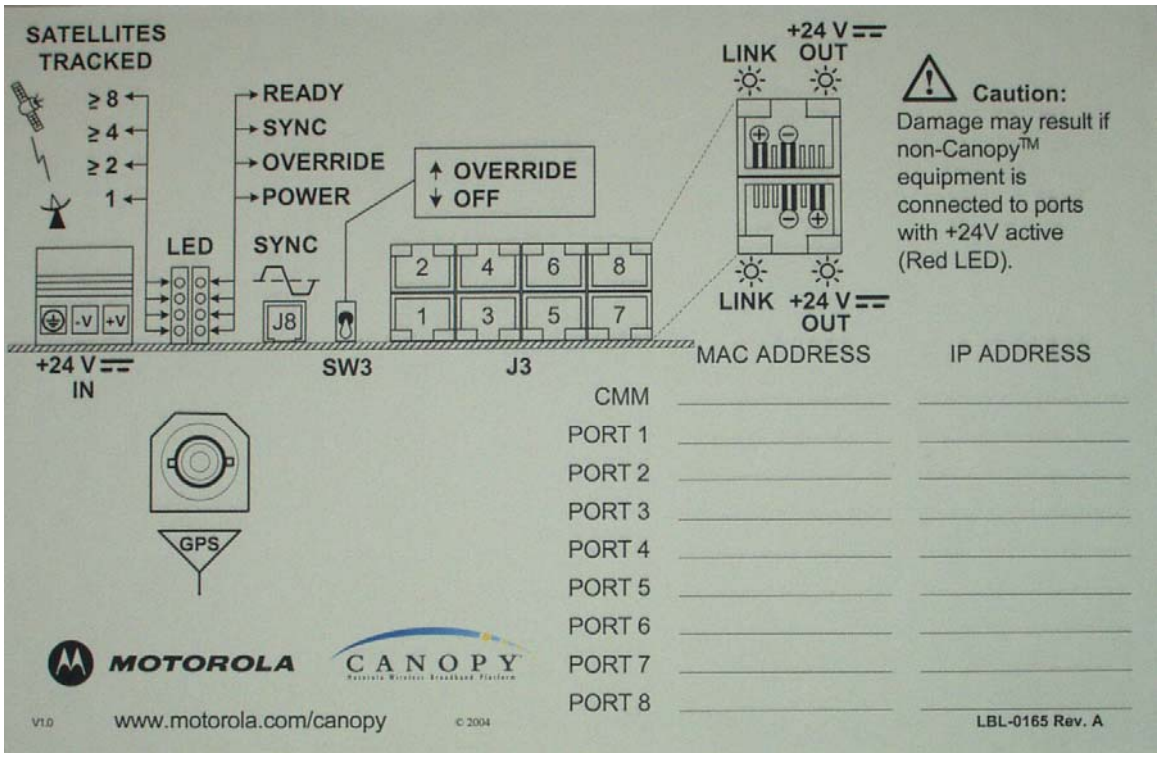
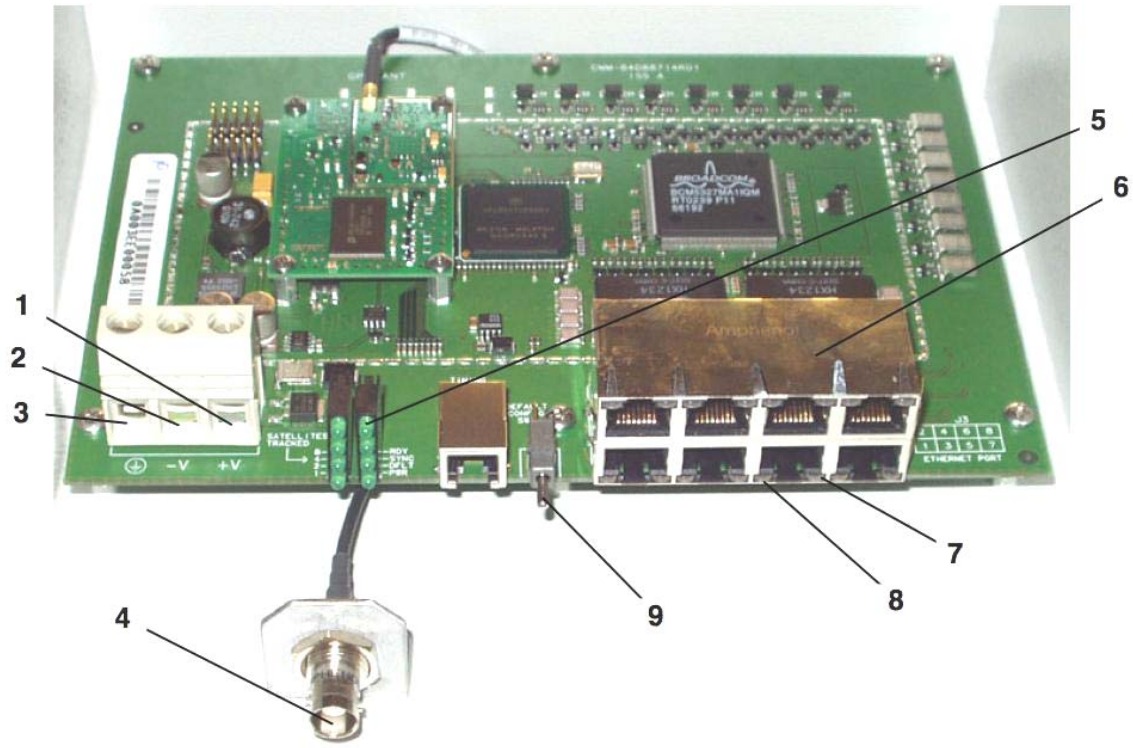


Figure 63: CMMmicro door label



1 **24 V DC power connection on terminal block (+V).**
2 **24 V DC ground connection on terminal block (-V).**
3 **Ground bonding point for CMMmicro. Ground connection on terminal block, for grounding to Protective Earth (PE) ⏚.**
4 **Female BNC connector for connecting to coax cable from GPS antenna.**
5 **Status display of eight green LEDs. The left LEDs show the number of satellites visible to the CMMmicro (1, 2, ≥ 4, and ≥ 8), and the right LEDs show status:**
   - **RDY (Ready) – Flashing LED indicates CMMmicro software has booted and is operational. LED continues to flash during normal operation.**
   - **SYNC – Constant LED indicates CMMmicro is receiving signal from the GPS antenna and is able to derive sync.**
   - **DFLT (default) – Constant LED indicates CMMmicro has booted with Override Switch in down/override position, and therefore with default IP address (169.254.1.1) and no password.**
   - **PWR (power) – Constant LED indicates CMMmicro has power.**
6 **8-port Ethernet connection block with 2 LEDs per port indicating port status.**
7 **Constant red LED to the right of each port indicates the port is powered with 24 V DC (controlled by the CMMmicro Configuration page).**
8 **Constant green LED to the left of each port indicates the port is detecting Ethernet connectivity.**
9 **Override toggle switch, for overriding a lost or unknown IP address or password. Down is normal position, while rebooting in the up position brings the CMMmicro up with the default IP address (169.254.1.1) and no password required.**

Figure 64: CMMmicro circuit board

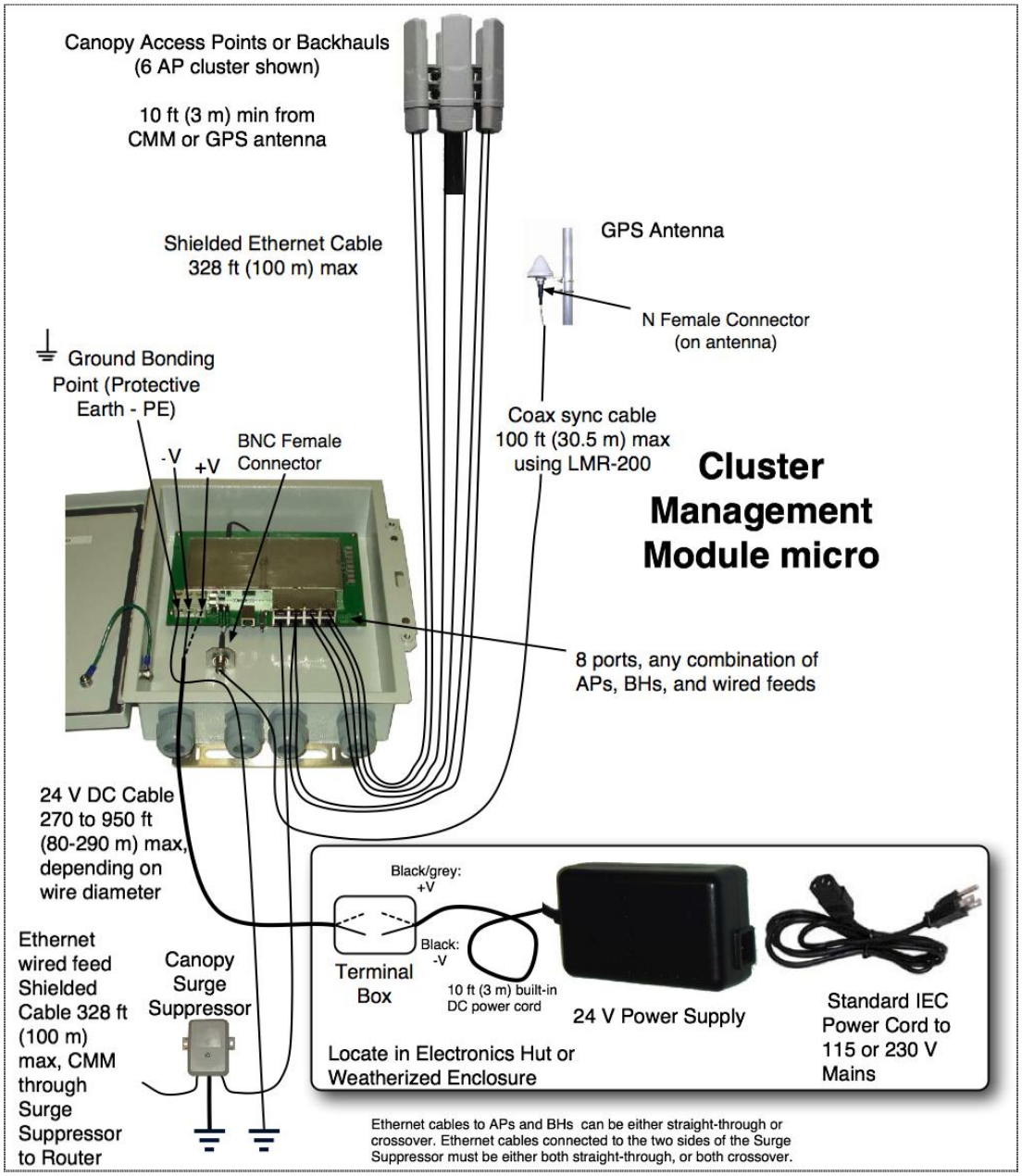


Figure 65: CMMmicro connections

16.4.8 Status Page of the CMMmicro

An example of a CMMmicro Status page is displayed in Figure 66.

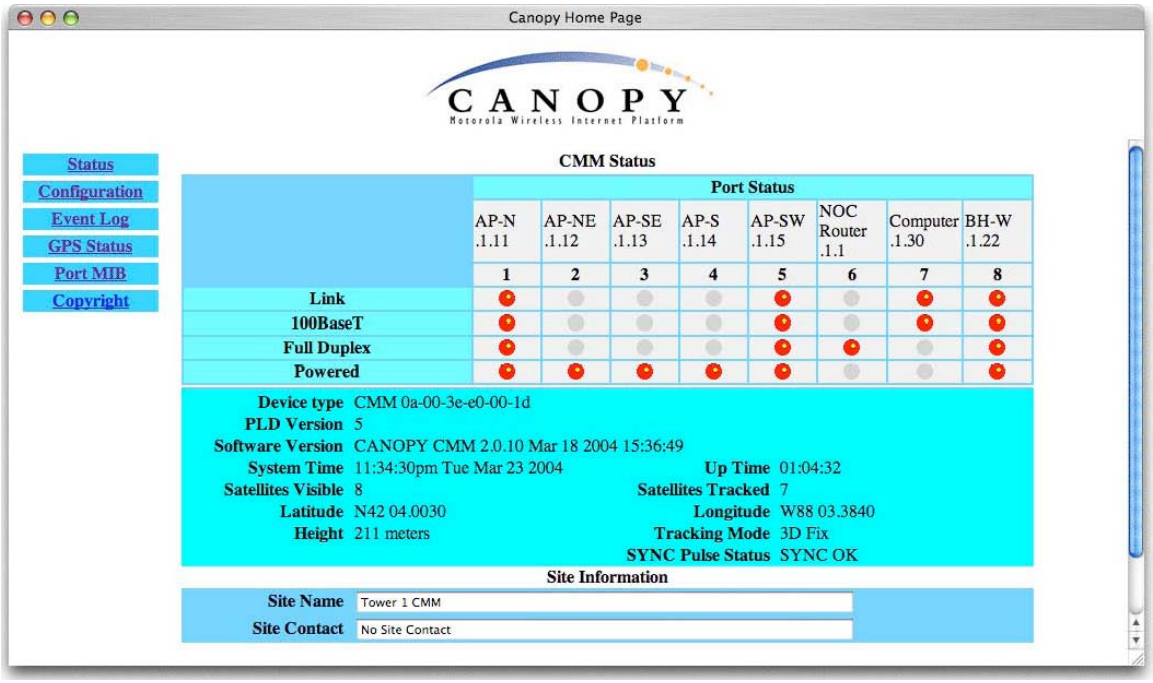


Figure 66: Status screen, CMMmicro

The Status page provides information on the operation of this CMMmicro. This is the default web page for the CMMmicro. The Status page provides the following fields.

Link

A red dot indicates that the port is active and detects Ethernet traffic. A grey dot indicates that the port is not active and no traffic is detected.

100BaseT

A red dot indicates that the port has auto-negotiated to a 100Base-T connection. A grey dot indicates that the port has auto-negotiated to a 10Base-T connection. (This convention is also used on many routers and network interface cards.) If the far end (an AP, a BH, a router) has been set to auto-negotiate, then the CMMmicro links at 100Base-T.

Full Duplex

A red dot indicates that the port has auto-negotiated to a Full Duplex connection. A grey dot indicates that the port has auto-negotiated to a Half Duplex connection. (This convention is also used on many routers and network interface cards.)

Powered

A red dot indicates that the port is powered with 24 V DC to provide power to an AP or BH. A grey dot indicates that the port is not powered. Port power is turned on and off in the **Port Power Control** parameter of the Configuration page. A CMMmicro comes from the factory with no Ethernet ports powered.

CAUTION!

Never connect any devices other than Canopy APs and BHs to a powered port. Powered ports are indicated by a red LED to the right of the port. (See Item 7 in Figure 64 on Page 172.) A powered port has 24-V DC on Pins 7 and 8 and 24-V return on Pins 4 and 5. This can damage other networking equipment, such as a computer or a router.

Device Type

This field displays the MAC address of the CMMmicro.

PLD Version

This field displays the version of the PLD (Programmable Logic Device) that is installed in the module. Before you request technical support, note this information.

Software Version

This field displays the version of the software that is installed in the module. Before you request technical support, note this information.

System Time

This field displays the current time. If the CMMmicro receives the signal from a GPS antenna, then this field expresses the time in Greenwich Mean Time (GMT).

Satellites Visible

This field displays how many satellites the GPS antenna sees.

NOTE:

This differs from the **Satellites Tracked** field (described below).

Latitude

If the CMMmicro receives the signal from a GPS antenna, then this field displays the latitude of the site.

Height

If the CMMmicro receives the signal from a GPS antenna, then this field displays the elevation (above sea level) of the GPS antenna.

Uptime

This field displays how much time has elapsed since the last boot of the CMMmicro.

Satellites Tracked

This field displays how many satellites the CMMmicro is tracking.

Longitude

If the CMMmicro receives the signal from a GPS antenna, then this field displays the longitude of the site.

Tracking Mode

If the CMMmicro receives the signal from a GPS antenna, then this field describes how the CMMmicro is tracking satellites.

Sync Pulse Status

This field indicates the status of sync pulse that the CMMmicro is currently able to provide to connected modules.

Site Name

This field displays administrative information that has been entered on the Configuration page of the CMMmicro.

Site Contact

This field displays administrative information that has been entered on the Configuration page of the CMMmicro.

16.4.9 Configuration Page of the CMMmicro

An example of the CMMmicro Configuration page is displayed in Figure 67.

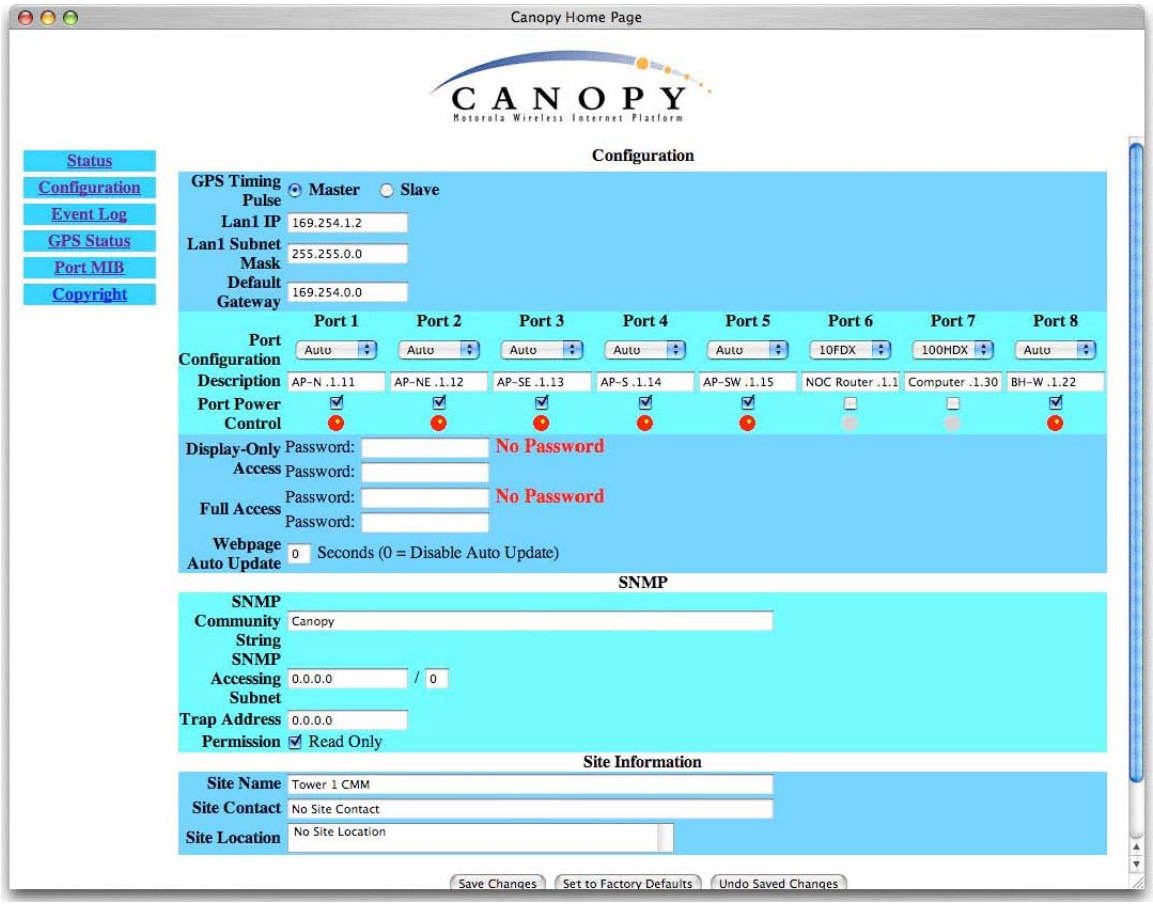


Figure 67: Configuration screen, CMMmicro

The Configuration web page contains all of the configurable parameters that define how the CMMmicro operates. The first line of information on the Configuration screen echoes the **Device Type** from the Status web page.

IMPORTANT!

Changes that are made to the following parameters become effective when you click the **Save Changes** button:

- **Port Configuration**
- **Description**
- **Power Port Control**
- **Webpage Auto Update**

When these parameters listed above have become effective, if you click the **Undo Saved Changes** button, the previous values *are not* restored.

Changes that are made to all other parameters become effective only after all of the following have occurred:

- you have clicked the **Save Changes** button.
- you click the **Reboot** button.
- the CMMmicro reboots.

Procedure 22: Setting CMMmicro parameters for test

To continue the test setup, configure

1. the **GPS Timing Pulse** parameter.
2. the **Lan1 IP** parameter.
3. the **Lan1 Subnet Mask** parameter.
4. the **Default Gateway** parameter.
5. the **Port Power Control** parameter.

end of procedure

GPS Timing Pulse

Select **Master**. (**Slave** is for future use.)

IMPORTANT!

If the GPS Timing Pulse is set to **Slave**, the CMMmicro GPS receiver is disabled.

Lan1 IP

Enter the IP address to be associated with the Ethernet connection on this CMMmicro. The default address is 169.254.1.1. If you set and then forget this parameter, then you must both

1. physically access the module.
2. use the CMMmicro override toggle switch to electronically access the module configuration parameters at 169.254.1.1. See Overriding Forgotten IP Addresses or Passwords on CMMmicro on Page 302.

RECOMMENDATION:
Note or print the IP settings from this page. Ensure that you can readily associate these IP settings both with the module and with the other data that you store about the module.

LAN Subnet Mask

Enter the appropriate subnet mask for the module to communicate on the network. The default value for this parameter is 255.255.0.0.

Default Gateway

Enter the appropriate gateway for the module to communicate on the network. The default for this parameter is 169.254.0.0.

Port Configuration

If you wish to force a port to a speed or duplex state, or to return the module to auto-negotiating speed and duplex state, change the selection for the port. The range of selections are defined in Table 38.

Table 38: Port Configuration selections for CMMmicro

Selection	Result
Auto	The port attempts to auto-negotiate speed and duplex state. (This is the default and recommended setting.)
100FDX	The port is forced to 100 Mbps and full duplex.
100HDX	The port is forced to 100 Mbps and half duplex.
10FDX	The port is forced to 10 Mbps and full duplex.
10HDX	The port is forced to 10 Mbps and half duplex.

If you change this value for a port and then click **Save Changes**, then the change becomes effective immediately and the previous value is lost.

Description

You can enter text in this parameter (for example, text that helps you to associate the port number with the connected device.) If you change this value for a port and then click

Save Changes, then the change becomes effective immediately and the previous value is lost.

Power Port Control

Ensure that power is off for every port that connects to a router, computer, or other network equipment. Turn on 24-V DC power for ports that connect to Canopy APs or BHs.

CAUTION!

Never connect any devices other than Canopy APs and BHs to a powered port. Powered ports are indicated by a red LED to the right of the port. (See Item 7 in Figure 64 on Page 172.) A powered port has 24-V DC on Pins 7 and 8 and 24-V return on Pins 4 and 5. This can damage other networking equipment, such as a computer or a router.

If you change this value for a port and then click **Save Changes**, then the change becomes effective immediately and the previous value is lost.

Display-Only Access

If you set (populate) the **Display-Only Access** password, this password will allow only *viewing* activities on the module.

This protection interacts with the **Full Access** password protection as follows:

- If the **Display-Only Access** password is set and the **Full Access** password *is not*, then the **Display-Only Access** password allows
  - telnet and FTP access to the module.
  - *viewing or changing* the parameters of the module. This configuration *is not* recommended.
- If the **Full Access** password is also set, then the **Full Access** password allows telnet and FTP access to the module, and the **Display-Only Access** password does not.
- If the **Display-Only Access** password *is not* set and the **Full Access** password is, then no password is required to view the parameters of the module.
- If neither password is set, then anyone can *view or change* the parameters of the module. This configuration *is not* recommended.

To set this password, enter the same expression in both **Display-Only Access** fields for verification. When the web-based interface prompts for this password, no user name is required. However, when a telnet or FTP session prompts for this password, you must enter the user name `root` in addition to the password.

If you set and then forget the **Display-Only Access** password, then you must both

physically access the module.

1. use the CMMmicro override toggle switch to electronically access the module configuration parameters at 169.254.1.1. See Overriding Forgotten IP Addresses or Passwords on CMMmicro on Page 302.

Full Access

If you set the **Full Access** password, this password will allow

- telnet and FTP access to the module.
- *viewing or changing* the parameters of the module.

To set this password, enter the same expression in both **Full Access** fields for verification. When the web-based interface prompts for this password, no user name is required. However, when a telnet or FTP session prompts for this password, you must enter the user name `root` in addition to the password.

If you set and then forget the **Full Access** password, then you must both

1. physically access the module.
2. use the CMMmicro override toggle switch to electronically access the module configuration parameters at 169.254.1.1. See Overriding Forgotten IP Addresses or Passwords on CMMmicro on Page 302.

NOTE:
You can unset either password (revert the access to no password required). To do so, type a space into the field and reboot the module. You must enter any password twice to allow the system to verify that the password is not mistyped. After any password is set and a reboot of the module has occurred, a **Password Set** indicator appears to the right of the field.

RECOMMENDATION:
Note the passwords that you enter. Ensure that you can readily associate these passwords both with the module and with the other data that you store about the module.

Webpage Auto Update

Enter the frequency (in seconds) for the web browser to automatically refresh the web-based interface. The default setting is 0. The 0 setting causes the web-based interface to never be automatically refreshed.

If you change this value and then click **Save Changes**, then the change becomes effective immediately and the previous value is lost.

SNMP Community String

Specify a control string that allows an Network Management Station (NMS) to access SNMP information. No spaces are allowed in this string. The default string is **Canopy**.

The **SNMP Community String** value is clear text and is readable by a packet monitor. Additional security derives from the configuration of the **SNMP Accessing Subnet**, **Trap Address**, and **Permission** parameters.

SNMP Accessing Subnet

Specify the addresses that are allowed to send SNMP requests to this CMMmicro. The NMS has an address that is among these addresses (this subnet). You must enter both

- The network IP address in the form xxx.xxx.xxx.xxx
- The CIDR (Classless Interdomain Routing) prefix length in the form /xx

For example

- the /16 in 198.32.0.0/16 specifies a subnet mask of 255.255.0.0 (the first 16 bits in the address range are identical among all members of the subnet).
- 192.168.102.0 specifies that any device whose IP address is in the range 192.168.102.0 to 192.168.102.254 can send SNMP requests to the CMMmicro, presuming that the device supplies the correct **SNMP Community String** value.

RECOMMENDATION:
For more information on CIDR, execute an Internet search on “Classless Interdomain Routing.”

The default treatment is to allow all networks access.

Trap Address

Specify the IP address (xxx.xxx.xxx.xxx) of a Network Management Station (NMS) to which trap information should be sent. Trap information informs the monitoring system that something has occurred. For example, trap information is sent

- after a reboot of the module.
- when an NMS attempts to access agent information but either
  - supplied an inappropriate community string or SNMP version number.
  - is associated with a subnet to which access is disallowed.

Permission

Select **Read Only** if you wish to disallow any parameter changes by the NMS.

Site Name

Specify a string to associate with the physical module. This parameter is written into the *sysName* SNMP MIB-II object and can be polled by an NMS. The buffer size for this field is 128 characters.

Site Contact

Enter contact information for the module administrator. This parameter is written into the *sysContact* SNMP MIB-II object and can be polled by an NMS. The buffer size for this field is 128 characters.

Site Location

Enter information about the physical location of the module. This parameter is written into the *sysLocation* SNMP MIB-II object and can be polled by an NMS. The buffer size for this field is 128 characters.

The CMMmicro Configuration page also provides the following buttons.

Save Changes, Undo Saved Changes, Set to Defaults, Reboot

The effects of clicking these buttons are defined in Table 39.

Table 39: When Changes Become Effective in CMMmicro

For these parameters…	clicking this button…	has this effect.
Port Configuration Description Power Port Control Webpage Auto Update	**Save Changes**	Any change becomes effective immediately and any previous setting is lost.
	Undo Saved Changes	No change is undone, and no previous setting is restored.
	Set to Defaults	The default setting is not restored.
	Reboot	No change that is not already effective becomes effective.
Any other parameter	**Save Changes**	Any change is recorded into flash memory but does not become effective immediately, and any previous setting can be restored.
	Undo Saved Changes	Any change recorded into flash memory is undone, and the previous setting is restored.
	Set to Defaults	The default setting is restored.
	Reboot	Any change recorded in flash memory (and not later undone) becomes effective.

In addition, when you click **Reboot**, the following events occur and are logged:

- The CMMmicro reboots.
- Any AP or BH that receives power from the CMMmicro loses power and thus also reboots.
- Any AP or BH that does not receive power but receives sync from the CMMmicro loses and then regains sync.

16.4.10 Configuring Modules for Connection to CMMmicro

After configuring the CMMmicro, configure the APs and BHs as follows. In each AP or BH that connects to a CMMmicro, you must set the **Sync Input** parameter of the Configuration page of that module to **Sync to Received Signal (Power Port)**.
See

- Sync Input on Page 190.
- Sync Input on Page 237.

16.4.11 Event Log Page of the CMMmicro

This page may contain information that can be useful under the guidance of Canopy technical support. For this reason, the operator should not clear the contents of this page before contacting technical support.

16.4.12 GPS Status Page of the CMMmicro

An example of the CMMmicro GPS Status page is displayed in Figure 68.

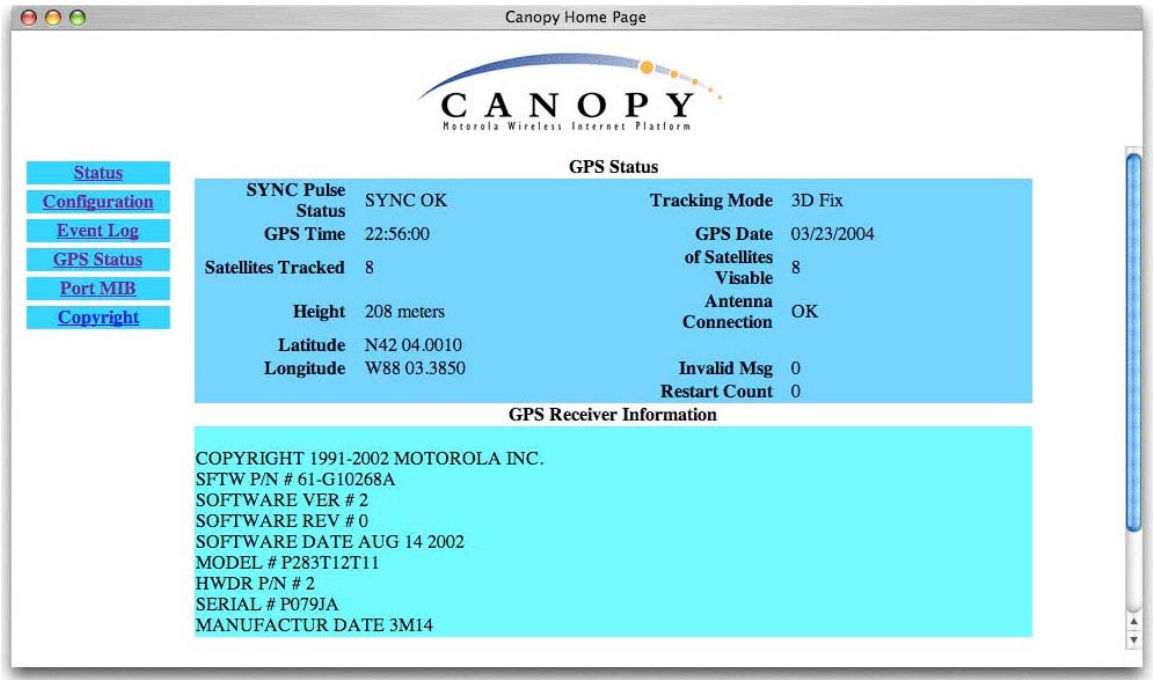


Figure 68: GPS Status screen, CMMmicro

The GPS Status page provides information from the GPS antenna and information about the GPS receiver in the CMMmicro.

Antenna Connection

This field displays the status of the signal from the antenna as follows:

- **OK** indicates that the GPS interface board is detecting an incoming signal on the coaxial cable from the GPS antenna.
- **No Antenna** indicates the GPS interface board is not detecting any incoming signal.

The other GPS Status fields are described under Satellites Visible on Page 175.

GPS Receiver Information

This field displays information about the GPS interface board.

16.4.13 Port MIB Page of the CMMmicro

An example of the Port MIB (Ethernet statistics) web page is displayed in Figure 69.

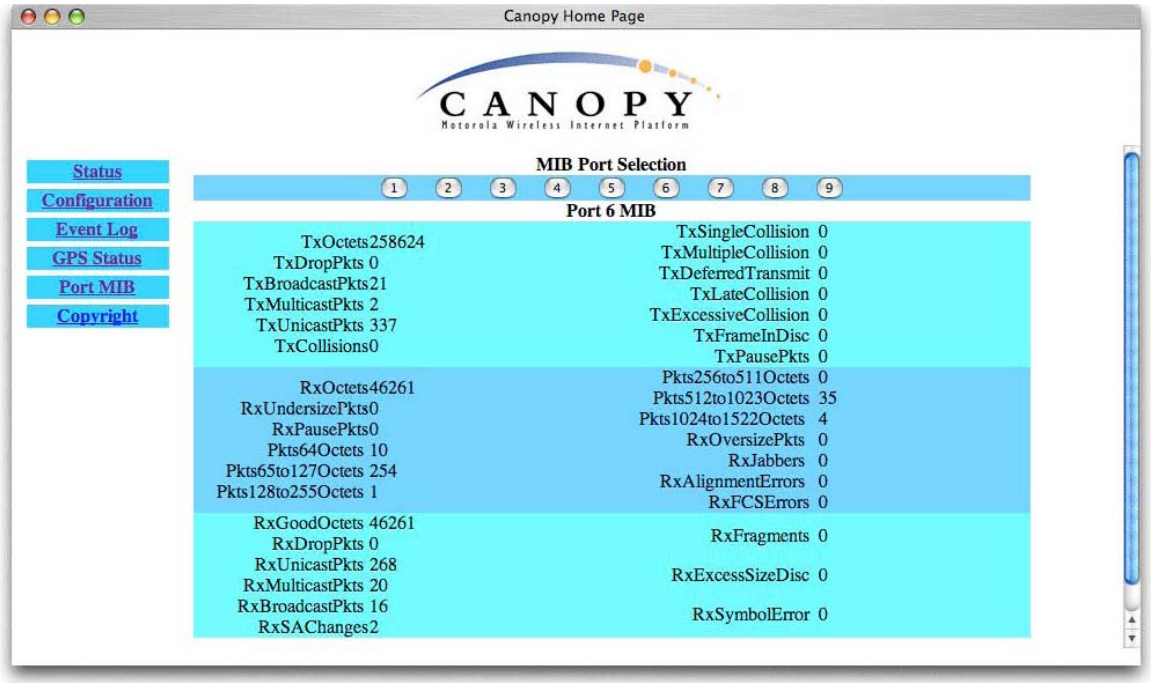


Figure 69: Port MIB screen, CMMmicro

The Port MIB page displays Ethernet statistics and traffic information for the ports on the managed switch. To display the port statistics, click on a port number.

Ports 1 through 8 are the regular ports, connected to APs, BHs, or other network elements. Port 9 is the connection between the managed switch and the CMMmicro processor. Thus, updates to interface pages, SNMP activities, and FTP and telnet sessions create traffic on Port 9.

These Ethernet statistics can also be retrieved from the CMMmicro by a Network Management Station using SNMP. During advanced troubleshooting, this information can be useful as you see the activity on a single port or as you compare activity between ports of the CMMmicro.

17 PREPARING COMPONENTS FOR DEPLOYMENT

Your test of the modules not only verified that they are functional, but also yielded data that you have stored about them. Most efficiently preparing modules for deployment involves

- retrieving that data.
- systematically collecting the data into a single repository, while keeping a strong (quick) association between the data and the module.
- immediately merging module access data into this previously stored data.

17.1 CORRELATING COMPONENT-SPECIFIC INFORMATION

You can use the data that you noted or printed from the Status pages of the modules to

- store modules for future deployment.
- know, at a glance, how well-stocked you are for upcoming network expansions.
- efficiently draw modules from stock for deployment.
- plan any software updates that you
  - wish to perform to acquire features.
  - need to perform to have the feature set be consistent among all modules in a network expansion.

You can make these tasks even easier by collecting this data into a sortable database.

17.2 ENSURING CONTINUING ACCESS TO THE MODULES

As you proceed through the steps under Configuring for the Destination on Page 189, you will set values for parameters that specify the sync source, data handling characteristics, security measures, management authorities, and other variables for the modules. While setting these, you will also tighten access to the module, specifically in

- the **Color Code** parameter of Configuration page
- the **Display-Only Access** and **Full Access** password parameters of the Configuration page.
- the addressing parameters of the IP Configuration page.

Before you set these, consider whether and how you may want to set these by a self-devised scheme. A password scheme can help you when you have forgotten or misfiled a password. An IP addressing scheme may be essential to the operation of your network and to future expansions of your network.

As you set these, note the color code and the passwords, and note or print the parameters you set on the IP Configuration page. Immediately associate them with the following previously stored data about the modules:

- device type, which includes the frequency band and MAC address
- software version, which includes the encryption type
- software boot version
- FPGA version, which also includes the encryption type

When you have the color code, passwords, and IP addressing readily available in the future, you will be able to access the module pages without physically accessing the module.

18 CONFIGURING FOR THE DESTINATION

18.1 CONFIGURING AN AP FOR THE DESTINATION

18.1.1 Configuration Page of the AP

An example of an AP Configuration screen is displayed in Figure 70.

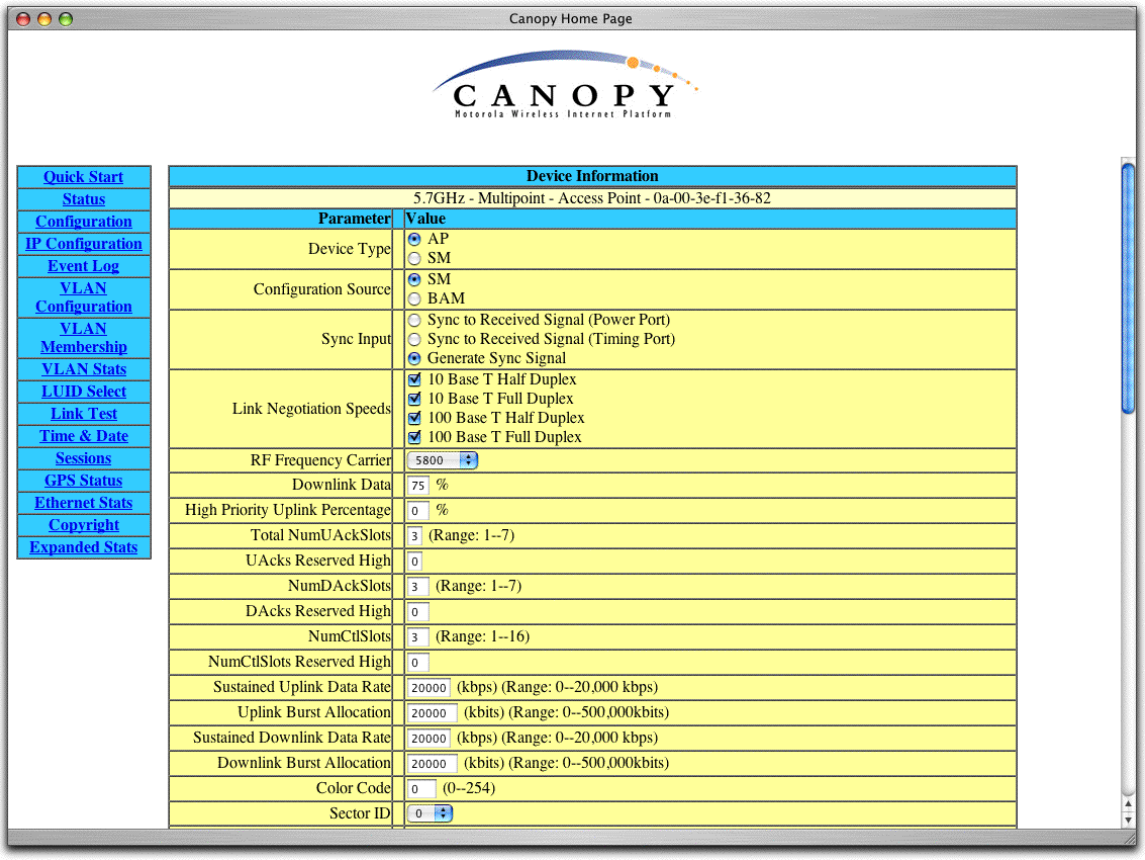


Figure 70: Configuration screen (top), AP

The Configuration web page contains all of the configurable parameters that define how the module operates. The first line of information on the Configuration screen echoes the **Device Type** from the Status web page.

You may set the Configuration page parameters as follows.

Sync Input

Specify the type of synchronization for this AP to use:

- Select **Sync to Received Signal (Power Port)** to set this AP to receive sync from a connected CMMmicro.
- Select **Sync to Received Signal (Timing Port)** to set this AP to receive sync from a connected CMM2, an AP in the cluster, an SM, or a BH timing slave.
- Select **Generate Sync Signal** where the AP does not receive sync, and no other AP or BHM is active within the link range. For link range information, see
  - AP-SM Link Distances on Page 73.
  - BH-BH Link Distances on Page 76.

Link Negotiation Speeds

Specify the type of link speed for the Ethernet connection. The default for this parameter is that all speeds are selected. The recommended setting is a single speed selection for all APs, BHs, and SMs in the operator network.

RF Frequency Carrier

Specify the frequency for the module to transmit. The default for this parameter is **None**. (The selection labeled **Factory** requires a special software key file for implementation.) For a list of channels in the band, see Considering Frequency Band Alternatives on Page 100.

Broadcast Repeat Count

In Release 4.2 and later releases, this parameter controls how many times, in addition to the original broadcast, the AP repeats each broadcast. Examples of conditions where each setting can be best are provided in the following table.

Value (retries)	Condition
0[1]	Where packet throughput is more important than reliability (such as in downstreaming video.
1[1]	
2[2]	Where the AP *does not* broadcast a significant amount of traffic.
3	Where a high rate of connectionless, unacknowledged packets (such as UDP) are transmitted (for example, where most broadcast traffic is in ARP).

NOTES:

1. If you configure the AP either to not rebroadcast or to rebroadcast only once, monitor transmissions to confirm that acceptable quality is achieved.
2. The previous and current default treatment is two retries.

Downlink Data

Specify the percentage of the aggregate throughput for the downlink (frames transmitted from the AP to the subscriber). For example, if the aggregate (uplink and downlink total) throughput on the AP is 6 Mb, then 75% specified for this parameter allocates 4.5 Mb for the downlink and 1.5 Mb for the uplink. The default for this parameter is 75%.

CAUTION!
You must set this parameter exactly the same for all APs in a cluster.

High Priority Uplink Percentage

Specify the percentage of the uplink bandwidth to dedicate to low-latency traffic. When set, this percentage of RF link bandwidth is permanently allocated to low-latency traffic, regardless of the amount of low-latency traffic that is present. No corresponding downlink parameter is settable. Scheduling algorithms in the AP allocate the corresponding downlink percentage.

IMPORTANT!
Carefully consider parameter settings for the high-priority channel. The bandwidth that you allocate to this channel decreases bandwidth on the regular channel, regardless of whether high-priority traffic exists. See High-priority Bandwidth on Page 64.

Wherever you wish to implement the high-priority channel, you must set *all* high-priority parameters. If all are not set, then the high-priority channel is not active.

Slot Specifications

The recommended settings for slot specification parameters are provided in Table 40.

Table 40: Slot settings for all APs in cluster, based on traffic type

Parameter	Recommended Setting[1]	
	***Without* High-priority Channel Enabled**	***With* High-priority Channel Enabled[2]**
Total NumUAckSlots	3	6
UAcks Reserved High	0	3
NumDAckSlots	3	6
DAcks Reserved High	0	3
NumCtlSlots	3[3]	6[4]
NumCtlSlots Reserved High	0	3

NOTES:

1. To avoid self-interference, for each of these six parameters, the value *must be* identical in all APs in a cluster.
2. Presumes that equipment is configured to set the low-latency ToS bit.
3. Where congestion occurs from the control overhead in predominantly small packets, setting this parameter to 4 may be better.
4. Where congestion occurs from the control overhead in predominantly small packets, setting this parameter to 7 may be better.

With Hardware Scheduler, the recommended number of control slots is as stated in Table 41.

Table 41: Control slot settings for all APs in cluster with Hardware Scheduler

Number of SMs that Register to the AP	Number of Control Slots Recommended
1 to 10	0
11 to 50	1
51 to 150	2
151 to 200	3

With Software Scheduler, the recommended number of control slots reverts to what is stated in Table 40.

Total NumUAckSlots

Specify how many slots to use to acknowledge data that an SM receives. The default value of this parameter is 3. See Slot Specifications above.

Uacks Reserved High

Specify how many slots to use to acknowledge high-priority data that an SM receives. The default value of this parameter is 0. See Slot Specifications above.

NumDAckSlots

Specify how many slots are used to acknowledge data that the AP receives. The default value of this parameter is 3. See Slot Specifications above.

Dacks Reserved High

Specify how many slots to use to acknowledge high-priority data that the AP receives. The default value of this parameter is 0. See Slot Specifications above.

NumCtlSlots

Specify how many slots to use to send control messages to an AP. The default value of this parameter is 3. See Slot Specifications above.

NumCtlSlots Reserved High

Specify how many slots to use to send control messages to an AP. You should set this parameter only when you implement the high-priority channel. The default value of this parameter is 0. See Slot Specifications above.

RECOMMENDATION:
See the description of interactions between sustained and burst data settings for the following parameters—Interaction of Burst Allocation and Sustained Data Rate Settings on Page 64.

Sustained Uplink Data Rate

Specify the rate at each SM registered to this AP is replenished with credits for transmission. The default rate is 20,000 kbps (in Release 6.1). This default imposes no restriction on the uplink.

Uplink Burst Allocation

Specify the maximum amount of data to allow each SM to transmit before being recharged with credits to transmit more. The default amount is 20,000 kb (in Release 6.1).

Sustained Downlink Data Rate

Specify the rate at which the AP to replenishes any registered SM with credits for reception. The default rate is 20,000 kbps (in Release 6.1). This default imposes no restriction on the uplink.

Downlink Burst Allocation

Specify the maximum amount of data to allow the AP to transmit to any registered SM before the SM is replenished with reception credits. The default amount is 20,000 kb (in Release 6.1).

Color Code

Specify a value from 0 to 254. For registration to occur, the color code of the SM and the AP *must* match. Color code is not a security feature. Instead, color code allows you to segregate an individual network or neighboring Canopy networks.

Color code also allows you to force an SM to register to only a specific AP, even where the SM can reach multiple APs. On all Canopy modules, the default setting for the color code value is 0. This value matches only the color code of 0 (*not* all 255 color codes).

RECOMMENDATION:
Note the color code that you enter. Ensure that you can readily associate this color code both with the module and with the other data that you store about the module.

Sector ID

Specify a number to associate with this AP. The Sector ID does not affect the operation of the AP. On the AP Eval Data web page of the SM, the **Sector ID** field identifies the AP that the SM sees. For efficient and accurate network management, you should

- assign a unique Sector ID to each sector in an AP cluster.
- repeat the assignment pattern throughout the entire Canopy system.

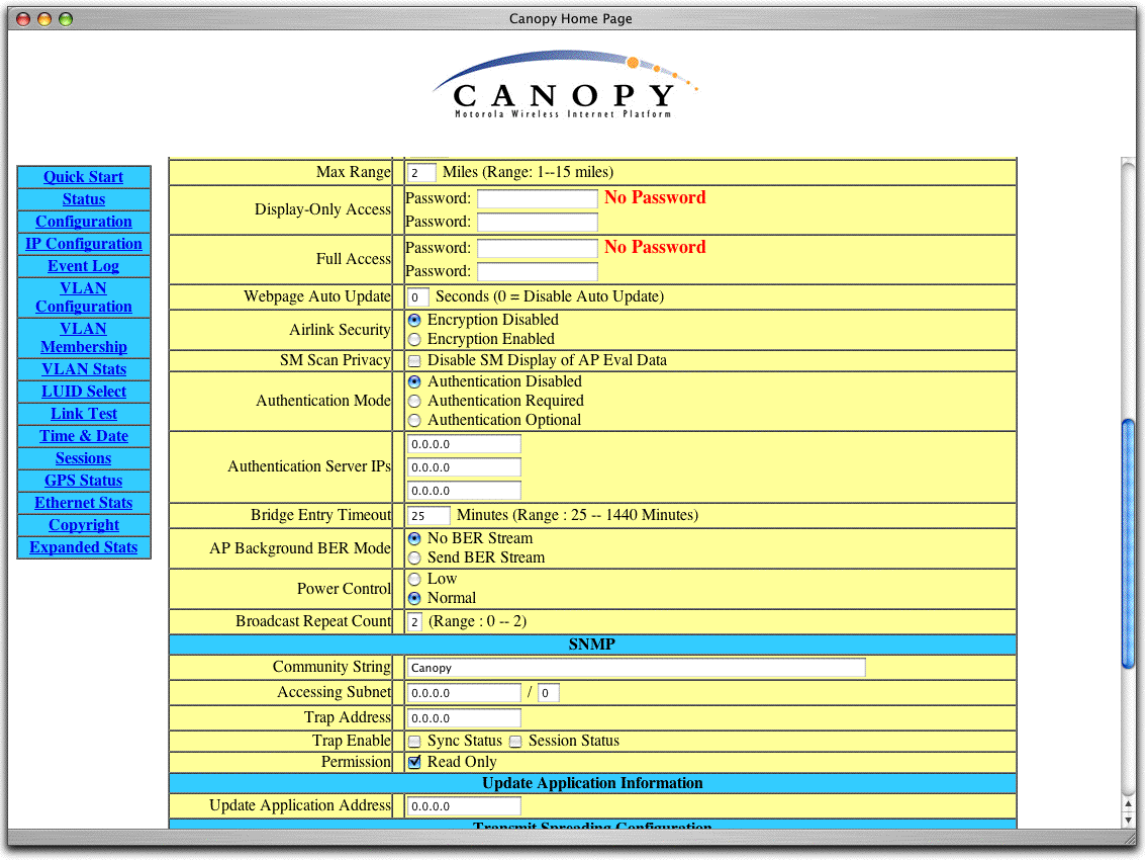


Figure 72: Configuration screen (middle), AP

As shown in Figure 72, the Configuration page continues.

Max Range

Enter a number of miles (or kilometers divided by 1.61, then rounded to an integer) for the furthest distance from which an SM is allowed to register to this AP. Do not set the distance to any greater number of miles. A greater distance

- does not increase the power of transmission from the AP.
- can reduce aggregate throughput.

Regardless of this distance, the SM must meet the minimum requirements for an acceptable link. If the AP is in cluster, then you *must* set this parameter on all other APs in the cluster exactly the same. The default value of this parameter is 2 miles (3.2 km).

In Release 4.2 and later releases for 2.4-GHz links, although the typical maximum range where an SM is deployed with a reflector is unchanged at 15 miles (24 km), you can set this parameter to as far as 30 miles (48 km). Without affecting the performance of the AP or SM, the greater value allows you to attempt the greater distance where the RF environment is uncontested and the Fresnel zone is clear.

NOTE:
A value of 15 for this parameter decreases the number of available data slots by 1.

External Filters Delay

Leave the value of this parameter set to 0, regardless of whether optional filters are installed.

Transmitter Output Power

Nations and regions may regulate transmitter output power. For example

- Both 900 MHz and 5.7 GHz modules come in connectorized versions, which require the operator to adjust power to ensure regulatory compliance. In addition to setting the power, the operator must set the “Antenna Gain – Cable Loss” so the module can accurately report received power at the antenna.
- Legal maximum allowable transmitter output power and EIRP (Equivalent Isotropic Radiated Power) in the 2.4 GHz frequency band varies by country and region. The output power of series 9 2.4 GHz modules can be adjusted to meet these national or regional regulatory requirements.
- Countries and regions that permit the use of the 5.4 GHz frequency band (CEPT member states, for example), generally require equipment using the band to have adjustable power.

The professional installer of Canopy equipment has the responsibility to

- maintain awareness of applicable regulations.
- calculate the permissible transmitter output power for the module.
- confirm that the initial power setting is compliant consistent with national or regional regulations.
- confirm that the power setting is compliant following any reset of the module to factory defaults.

For information on how to calculate the permissible transmitter output power to enter in this parameter, see Adjusting Transmitter Output Power on Page 255.

Display-Only Access

If you set (populate) the **Display-Only Access** password, this password will allow only *viewing* activities on the module.

This protection interacts with the **Full Access** password protection as follows:

- If the **Display-Only Access** password is set and the **Full Access** password *is not*, then the **Display-Only Access** password allows
  - telnet and FTP access to the module.
  - *viewing or changing* the parameters of the module. This configuration *is not* recommended.

- If the **Full Access** password is also set, then the **Full Access** password allows telnet and FTP access to the module, and the **Display-Only Access** password does not.
- If the **Display-Only Access** password *is not* set and the **Full Access** password is, then no password is required to view the parameters of the module.
- If neither password is set, then anyone can *view or change* the parameters of the module. This configuration *is not* recommended.

To set this password, enter the same expression in both **Display-Only Access** fields for verification. When the web-based interface prompts for this password, no user name is required. However, when a telnet or FTP session prompts for this password, you must enter the user name `root` in addition to the password.

If you set and then forget the **Display-Only Access** password, then you must both

1. physically access the module.
2. use an override plug to electronically access the module configuration parameters at 169.254.1.1. See Overriding Forgotten IP Addresses or Passwords on AP, SM, or BH on Page 302.

Full Access

If you set the **Full Access** password, this password will allow

- telnet and FTP access to the module.
- *viewing or changing* the parameters of the module.

To set this password, enter the same expression in both **Full Access** fields for verification. When the web-based interface prompts for this password, no user name is required. However, when a telnet or FTP session prompts for this password, you must enter the user name `root` in addition to the password.

If you set and then forget the **Full Access** password, then you must both

1. physically access the module.
2. use an override plug to electronically access the module configuration parameters at 169.254.1.1. See Overriding Forgotten IP Addresses or Passwords on AP, SM, or BH on Page 302.

NOTE:
You can unset either password (revert the access to no password required). To do so, type a space into the field and reboot the module. You must enter any password twice to allow the system to verify that the password is not mistyped. After any password is set and a reboot of the module has occurred, a **Password Set** indicator appears to the right of the field.

RECOMMENDATION:
Note the passwords that you enter. Ensure that you can readily associate these passwords both with the module and with the other data that you store about the module.

Webpage Auto Update

Enter the frequency (in seconds) for the web browser to automatically refresh the web-based interface. The default setting is 0. The 0 setting causes the web-based interface to never be automatically refreshed.

Airlink Security

Specify the type of air link security to apply to this AP:

- **Encryption Disabled** provides no encryption on the air link. This is the default mode.
- **Encryption Enabled** provides encryption, using a factory-programmed secret key that is unique for each module.

Encrypt Downlink Broadcast

In Release 4.2 or later release, when **Encryption Enabled** is selected in the **Airlink Security** parameter (described above) and **Enable** is selected in the **Encrypt Downlink Broadcast** parameter, the AP encrypts downlink broadcast packets as

- DES where the AP is DES capable.
- AES where the AP is AES capable.

CAUTION!

Do not select **Enable** for this parameter until all SMs that will register to this AP operate on Release 4.2 or a later release. An SM that operates on an earlier release cannot decrypt encrypted broadcasts and, consequently, drops connectivity (or cannot establish a link) with the AP that is configured to encrypt downlink broadcasts.

For more information about the Encrypt Downlink Broadcast feature, see Encrypting Downlink Broadcasts on Page 305.

SM Scan Privacy

When the SM Scan Privacy feature is enabled, you can use this field to suppress the display of data about this AP on the AP Eval Data page of all SMs that register.

Authentication Mode

If the AP has authentication capability, then you can use this field to select from among the following authentication modes:

- **Authentication Disabled**—the AP requires no SMs to authenticate.
- **Authentication Required**—the AP requires any SM that attempts registration to be authenticated in the BAM server before registration.
- **Authentication Optional**—the AP requires all SMs that attempt registration to be authenticated before registration, except any SM that is operating on a Canopy system release of earlier than Release 3.0. (These earlier releases *did not* support authentication for SMs.) *This value is not recommended.*

If the AP *does not* have authentication capability, then this parameter displays **Authentication Not Available**.

Authentication Server IPs

If the optional BAM server is implemented and the AP has authentication capability, enter the IP address of one or more BAM servers that perform authentication for SMs registered to this AP. Enter these in order of primary, secondary, then tertiary.

Bridge Entry Timeout

Specify the appropriate bridge timeout for correct network operation with the existing network infrastructure. The Bridge Entry Timeout should be a longer period than the ARP (Address Resolution Protocol) cache timeout of the router that feeds the network.

CAUTION!
An inappropriately low Bridge Entry Timeout setting may lead to temporary loss of communication with some end users.

AP Background BER Mode

Specify whether continuous BER (Bit Error Rate) data collection should be done. When **Send BER Stream** is selected for this parameter, you can read the bit error rate on the subscriber side to assess the quality of a registered link. However, two caveats apply to this setting:

- This parameter must be identically set for all APs in a cluster.
- When **Send BER Stream** is selected for this parameter, the aggregate available bandwidth decreases by approximately 200 kbps. For this reason, you should limit BER data collection to diagnostic intervals.

Power Control

In Release 4.1 and later releases, select either

- **Low** to set the AP to operate at 18 dB less than full power to reduce the possibility of self-interference with a nearby module.
- **Normal** to allow the AP to operate at full power.

CAUTION!
Selection of **Low** can cause the AP to drop an active RF link to an SM that is too far from the low-power AP. If a link is dropped when Power Control is set to **Low**, the link can be re-established by only Ethernet access.

If you select **Low** and save the changes and reboot the AP, you should immediately open the Link Test page and perform a link test.

Community String

Specify a control string that allows an Network Management Station (NMS) to access SNMP information. No spaces are allowed in this string. The default string is **Canopy**.

The **Community String** value is clear text and is readable by a packet monitor. Additional security derives from the configuration of the **Accessing Subnet**, **Trap Address**, and **Permission** parameters.

Accessing Subnet

Specify the addresses that are allowed to send SNMP requests to this AP. The NMS has an address that is among these addresses (this subnet). You must enter both

- The network IP address in the form xxx.xxx.xxx.xxx
- The CIDR (Classless Interdomain Routing) prefix length in the form /xx

For example

- the /16 in 198.32.0.0/16 specifies a subnet mask of 255.255.0.0 (the first 16 bits in the address range are identical among all members of the subnet).
- 192.168.102.0 specifies that any device whose IP address is in the range 192.168.102.0 to 192.168.102.254 can send SNMP requests to the AP, presuming that the device supplies the correct **Community String** value.

The default treatment is to allow all networks access. For more information on CIDR, execute an Internet search on “Classless Interdomain Routing.”

Trap Address

Specify the IP address (xxx.xxx.xxx.xxx) of a Network Management Station (NMS) to which trap information should be sent. Trap information informs the monitoring system that something has occurred. For example, trap information is sent

- after a reboot of the module.
- when an NMS attempts to access agent information but either
  - supplied an inappropriate community string or SNMP version number.
  - is associated with a subnet to which access is disallowed.

Trap Enable

Select either **Sync Status** or **Session Status** to enable SNMP traps. If you select neither, then traps are disabled.

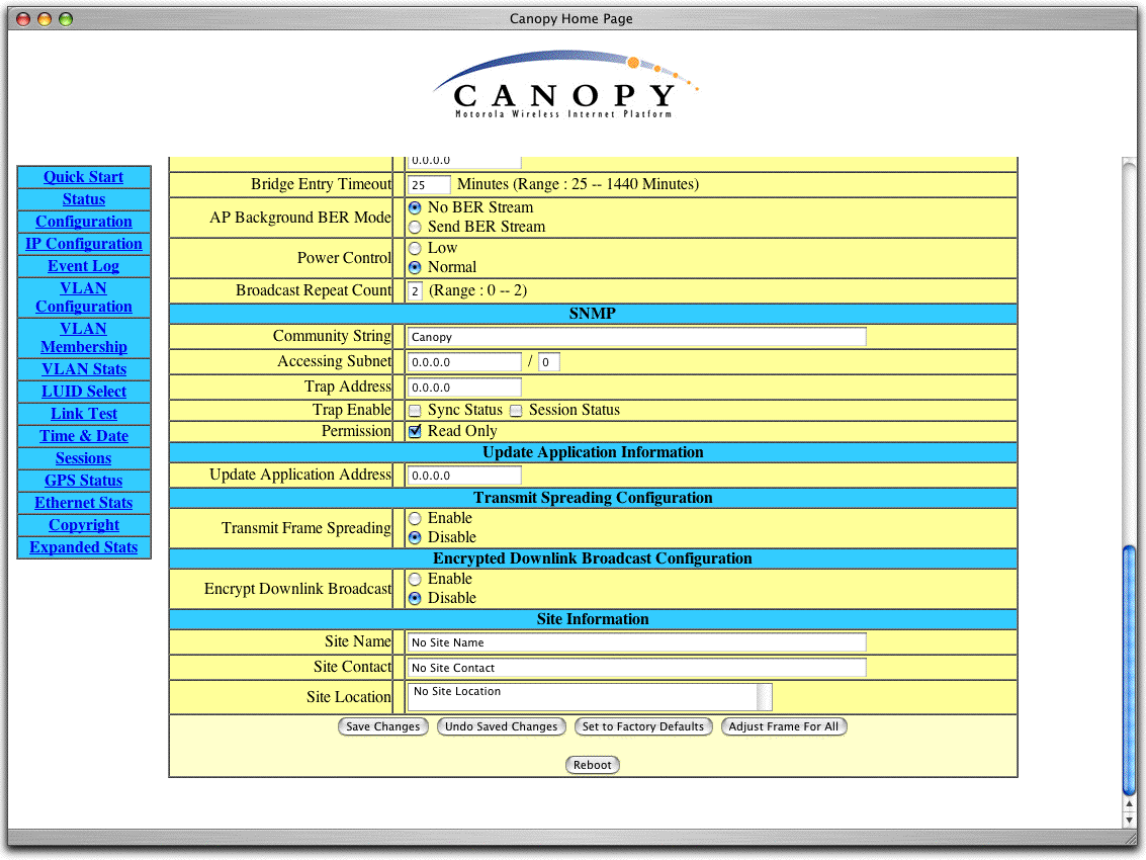


Figure 73: Configuration screen (bottom), AP

As shown in Figure 73, the AP Configuration page continues.

VLAN

Specify whether VLAN functionality for the AP and all linked SMs should (**Enable**) or should not (**Disable**) be allowed. The default value is **Disable**.

Dynamic Learning

Specify whether the AP should (**Enable**) or should not (**Disable**) add the VIDs of upstream frames to the VID table. (The AP passes frames with VIDs that are stored in the table both upstream and downstream.) The default value is **Enable**.

Allow Only Tagged Frames

Specify whether the AP should drop (**Enable**) frames that arrive without a tag at its wired Ethernet interface or should tag (**Disable**) those untagged frames using the VID that is stored in the **Management VID** parameter. The default value is **Disable**.

VLAN Aging Timeout

Specify how long the AP should keep dynamically learned VIDs. The range of values is 5 to 1440 (minutes). The default value is **25** (minutes).

NOTE:
VIDs that you enter for the **Management VID** and **VLAN Membership** parameters do not time out.

Management VID

Enter the VID that the operator wishes to use to communicate with the module manager. The range of values is 1 to 4095. The default value is **1**.

VLAN Membership

Enter the set of allowed VIDs for the AP. The range of values is 1 to 4095. The default value is **1**.

Permission

Select **Read Only** if you wish to disallow any parameter changes by the NMS.

Update Application Address

For capabilities in future software releases, you can enter the address of the server to access for software updates on this AP and registered SMs.

Transmit Frame Spreading

If you select **Enable**, then SMs between two APs can register in the assigned AP (do not register in another AP). Where all SMs operate on Release 4.0 or later

- and multiple AP clusters operate in the same frequency band range and same geographical area, select **Enable**.
- and multiple AP clusters *do not* operate in the same frequency band range and same geographical area, select **Disable**, but observe the following caveat.

IMPORTANT!
SM throughput is 10% greater with this feature disabled. However, if you disable Transmit Frame Spreading where this feature was previously enabled, monitor the zone for interference over a period of days to ensure that this action has not made SMs sensitive to the wrong beacons.

With this selection enabled, the AP does not transmit a beacon in each frame, but rather transmits a beacon in only pseudo-random frames in which the SM expects the beacon. This allows multiple APs to send beacons to multiple SMs in the same range without interference.

Site Name

Specify a string to associate with the physical module. This parameter is written into the *sysName* SNMP MIB-II object and can be polled by an NMS. The buffer size for this field is 128 characters.

Site Contact

Enter contact information for the module administrator. This parameter is written into the *sysContact* SNMP MIB-II object and can be polled by an NMS. The buffer size for this field is 128 characters.

Site Location

Enter information about the physical location of the module. This parameter is written into the *sysLocation* SNMP MIB-II object and can be polled by an NMS. The buffer size for this field is 128 characters.

The Configuration page also provides the following buttons.

Save Changes

When you click this button, any changes that you made on the Configuration page are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Undo Saved Changes

When you click this button, any changes that you made but were not committed by a reboot of the module are undone.

Set to Factory Defaults

When you click this button, *all configurable parameters on all configurable pages* are reset to the factory settings.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

Whenever you change a parameter in the Configuration page, the system highlights the **Reboot** button as a reminder that a reboot (in addition to a save) is required to implement the changes.

18.1.2 IP Configuration Page of the AP

An example of the AP IP Configuration screen is displayed in Figure 74.

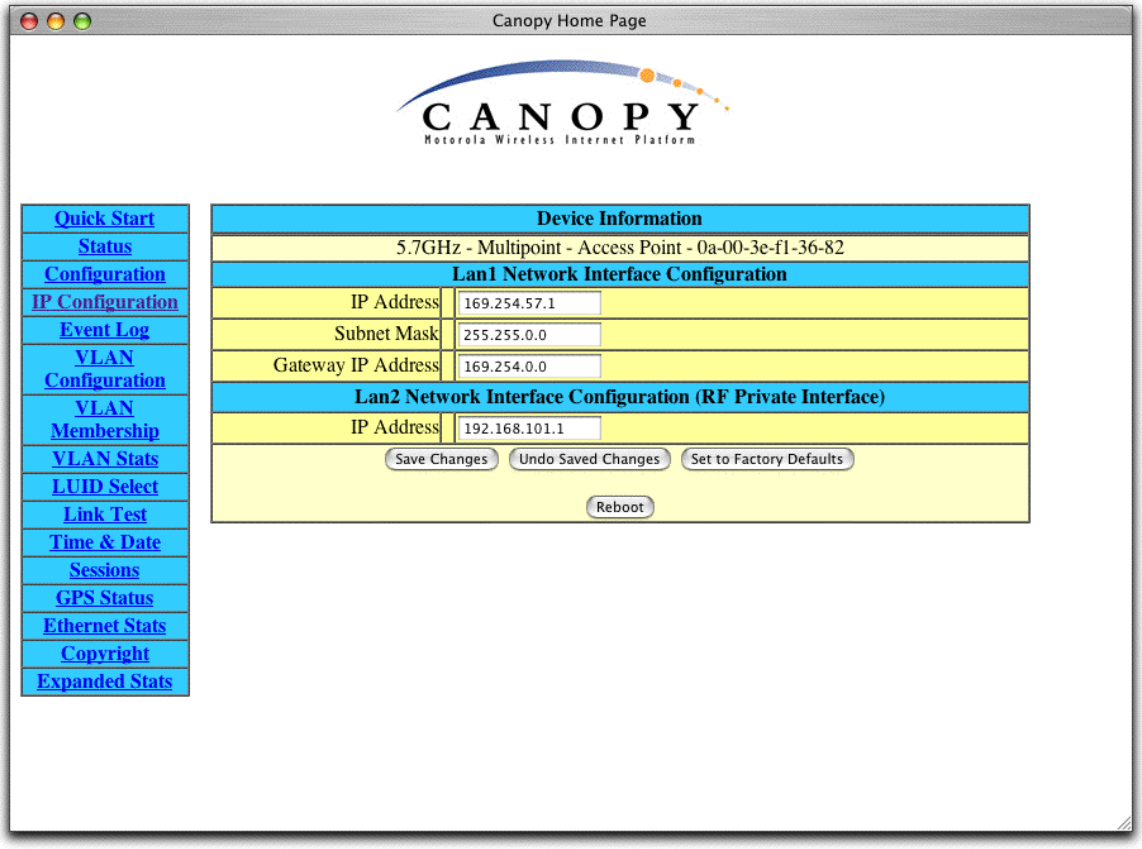


Figure 74: IP Configuration screen, AP

You may set the IP Configuration page parameters as follows.

LAN1 Network Interface Configuration, IP Address

Enter the *non-routable* IP address to associate with the Ethernet connection on this AP. (The default IP address from the factory is 169.254.1.1.) If you set and then forget this parameter, then you must both

1. physically access the module.
2. use an override plug to electronically access the module configuration parameters at 169.254.1.1. See Overriding Forgotten IP Addresses or Passwords on AP, SM, or BH on Page 302.

RECOMMENDATION:
Note or print the IP settings from this page. Ensure that you can readily associate these IP settings both with the module and with the other data that you store about the module.

LAN1 Network Interface Configuration, Subnet Mask

Enter an appropriate subnet mask for the AP to communicate on the network. The default subnet mask is 255.255.255.0. See Allocating Subnets on Page 123.

LAN1 Network Interface Configuration, Gateway IP Address

Enter the appropriate gateway for the AP to communicate with the network. The default gateway is 169.254.0.0.

LAN2 Network Interface Configuration (RF Private Interface), IP Address

You should not change this parameter from the default *AP* private IP address of 192.168.101.1. A flat Class C subnet is used to communicate with each of the SMs that are registered. The AP uses a combination of the private IP and the LUID (logical unit ID) of the SM.

For example, if an SM is the first to register in an AP, and another SM registers later, then the AP whose Private IP address is 192.168.101.1 uses the following *SM* Private IP addresses to communicate to each:

SM	LUID	Private IP
First SM registered	2	192.168.101.2
Second SM registered	3	192.168.101.3

If the private IP address of the *AP* is changed, then the new address must

- designate a Class C subnet that is not used for anything else.
- have the form xxx.xxx.xxx.1, where 1 is the value of the last octet of the address.

NOTE:
Where space is limited for subnet allocation, be advised that an SM *need not* have an operator-assigned IP address. The SM is directly accessible without an LUID if either the SM **Color Code** parameter is set to 0 or the AP has a direct Ethernet connection to the SM.

The IP Configuration page also provides the following buttons.

Save Changes

When you click this button, any changes that you made on the IP Configuration page are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Undo Saved Changes

When you click this button, any changes that you made but were not committed by a reboot of the module are undone.

Set to Factory Defaults

When you click this button, *all configurable parameters on all configurable pages* are reset to the factory settings.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

Whenever you change a parameter in the IP Configuration page, the system highlights the **Reboot** button as a reminder that a reboot (in addition to a save) is required to implement the changes.

18.2 CONFIGURING AN SM FOR THE DESTINATION

18.2.1 Configuration Page of the SM

An example of an SM Configuration screen is displayed in Figure 75.

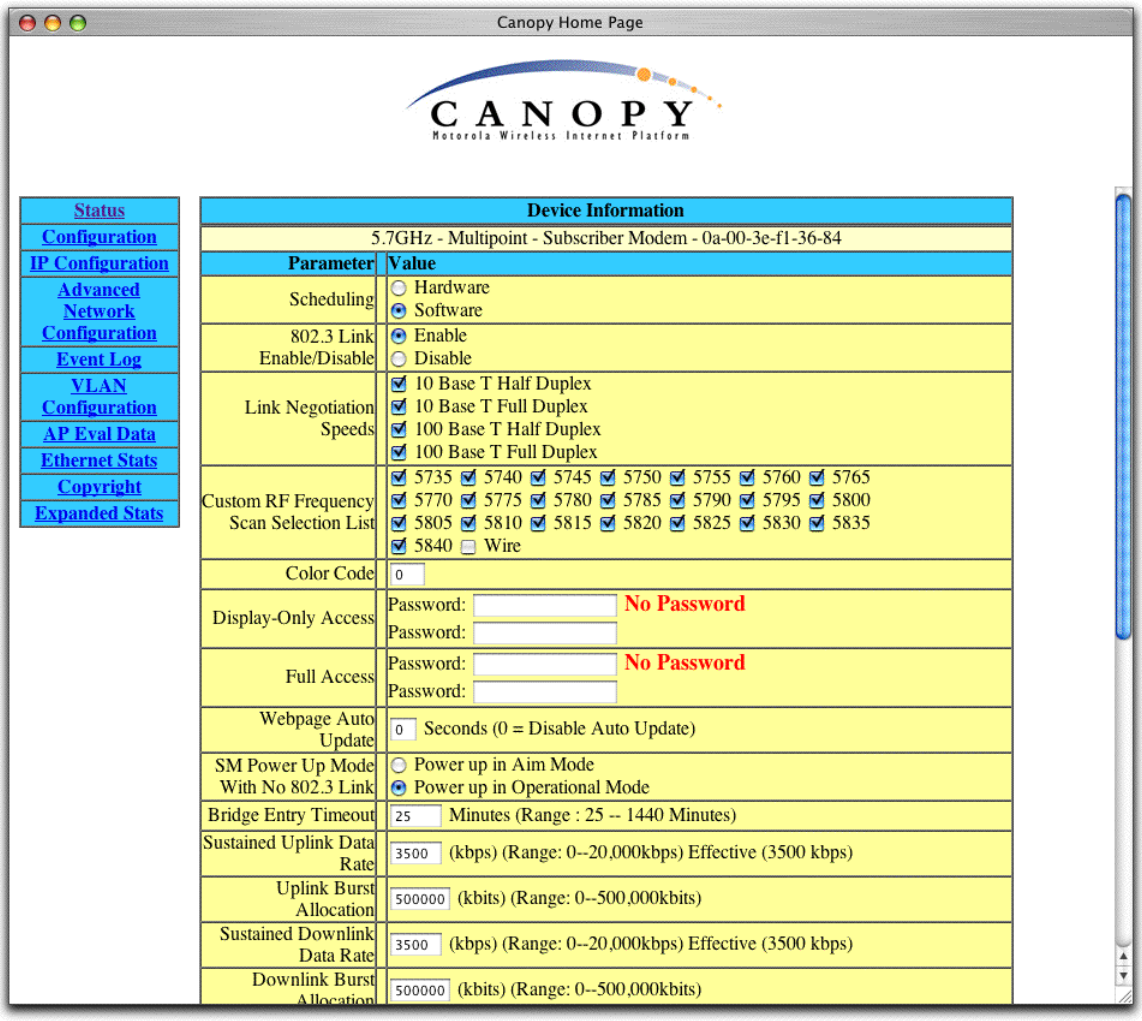


Figure 75: Configuration screen, SM

The Configuration web page contains all of the configurable parameters that define how the SM operates. The first line of information on the Configuration screen echoes the **Device Type** from the Status web page.

As shown in Figure 75, you may set the Configuration page parameters as follows.

802.3 Link Enable/Disable

Specify whether to disallow the SM to send and receive data through the Ethernet port even when the RF link to the AP is active. This parameter toggles on or off the Browser-based Disabling of Subscriber Module Ethernet Interface feature in Release 3.2 and later releases. You can alternatively control this feature from the AP.

When you select **Enable**, this feature

- disallows the SM user to access the link, as in the case where the user account is delinquent.
- allows the operator to partition the network for troubleshooting or another analytical or operational function.

When you select **Disable**, this feature is deactivated.

Link Negotiation Speeds

Specify the type of link speed for the Ethernet connection. The default for this parameter is that all speeds are selected. The recommended setting is a single speed selection for all APs, BHs, and SMs in the operator network.

Custom RF Frequency Scan Selection List

Specify the frequency that the SM scans to find the Access Point. The frequency *band* of the SM affects what channels you should select.

IMPORTANT!

In the 2.4-GHz frequency band, the SM can register to an AP that transmits on a frequency 2.5 MHz higher than the frequency that the SM receiver locks when the scan terminates as successful. This establishes a poor-quality link. To prevent this, select frequencies that are at least 5 MHz apart.

In a 2.4-GHz SM, this parameter displays all available channels, but has only three recommended channels selected by default. See 2.4-GHz AP Cluster Recommended Channels on Page 101.

In a 5.2- or 5.4-GHz SM, this parameter displays only ISM frequencies. In a 5.7-GHz SM, this parameter displays both ISM and U-NII frequencies. If you select all frequencies that are listed in this field (default selections), then the SM scans for a signal on any channel. If you select only one, then the SM limits the scan to that channel. Since the frequencies that this parameter offers for each of these two bands are 5 MHz apart, a scan of *all* channels does not risk establishment of a poor-quality link as in the 2.4-GHz band.

A list of channels in the band is provided in Considering Frequency Band Alternatives on Page 100.

(The selection labeled **Factory** requires a special software key file for implementation.)

Color Code

Specify a value from 0 to 254. For registration to occur, the color codes of the SM and of the AP *must* match. Color code is not a security feature. Instead, color code allows you to segregate an individual network or neighboring Canopy networks.

Color code also allows you to force an SM to register to only a specific AP, even if the SM can reach multiple APs. On all Canopy modules, the default setting for the color code value is 0. This value matches only the color code of 0 (*not* all 255 color codes).

RECOMMENDATION:
Note the color code that you enter. Ensure that you can readily associate this color code both with the module and with the other data that you store about the module.

Display-Only Access

If you set (populate) the **Display-Only Access** password, this password will allow only *viewing* activities on the module.

This protection interacts with the **Full Access** password protection as follows:

- If the **Display-Only Access** password is set and the **Full Access** password *is not*, then the **Display-Only Access** password allows
  - telnet and FTP access to the module.
  - *viewing or changing* the parameters of the module. This configuration *is not* recommended.
- If the **Full Access** password is also set, then the **Full Access** password allows telnet and FTP access to the module, and the **Display-Only Access** password does not.
- If the **Display-Only Access** password *is not* set and the **Full Access** password is, then no password is required to view the parameters of the module.
- If neither password is set, then anyone can *view or change* the parameters of the module. This configuration *is not* recommended.

To set this password, enter the same expression in both **Display-Only Access** fields for verification. When the web-based interface prompts for this password, no user name is required. However, when a telnet or FTP session prompts for this password, you must enter the user name `root` in addition to the password.

If you set and then forget the **Display-Only Access** password, then you must both

1. physically access the module.
2. use an override plug to electronically access the module configuration parameters at 169.254.1.1. See Overriding Forgotten IP Addresses or Passwords on AP, SM, or BH on Page 302.

Full Access

If you set the **Full Access** password, this password will allow

- telnet and FTP access to the module.
- *viewing or changing* the parameters of the module.

To set this password, enter the same expression in both **Full Access** fields for verification. When the web-based interface prompts for this password, no user name is required. However, when a telnet or FTP session prompts for this password, you must enter the user name `root` in addition to the password.

If you set and then forget the **Full Access** password, then you must both

1. physically access the module.
2. use an override plug to electronically access the module configuration parameters at 169.254.1.1. See Overriding Forgotten IP Addresses or Passwords on AP, SM, or BH on Page 302.

NOTE:
You can unset either password (revert the access to no password required). To do so, type a space into the field and reboot the module. You must enter any password twice to allow the system to verify that the password is not mistyped. After any password is set and a reboot of the module has occurred, a **Password Set** indicator appears to the right of the field.

RECOMMENDATION:
Note the passwords that you enter. Ensure that you can readily associate these passwords both with the module and with the other data that you store about the module.

Webpage Auto Update

Enter the frequency (in seconds) for the web browser to automatically refresh the web-based interface. The default setting is 0. The 0 setting causes the web-based interface to never be automatically refreshed.

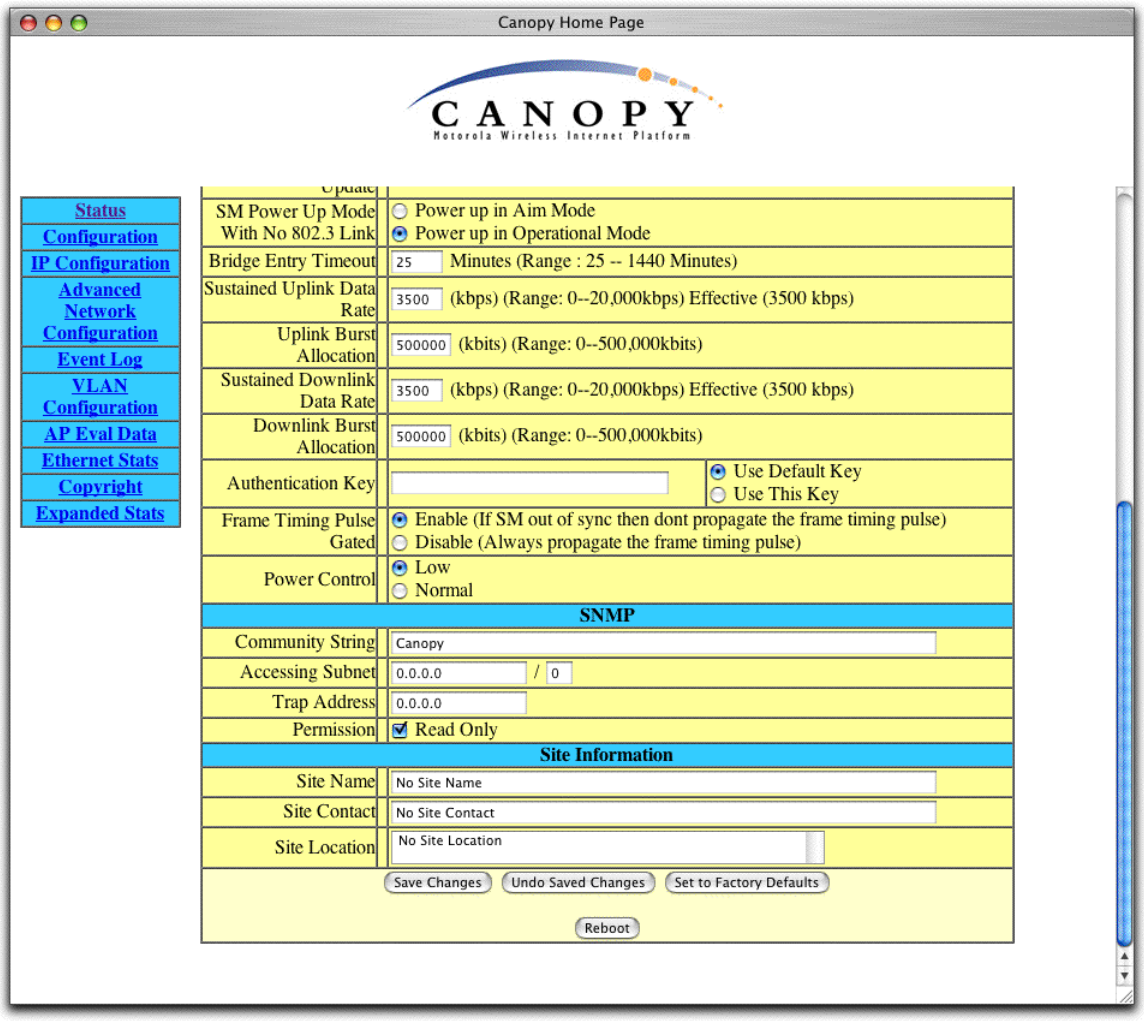


Figure 76: Configuration screen, SM (continued)

As shown in Figure 76, the Configuration page continues.

SM Power Up Mode With No 802.3 Link

Specify the default mode in which this SM will power up when the SM senses no Ethernet link. Select either

- **Power Up in Aim Mode**—the SM boots in an aiming mode. When the SM senses an Ethernet link, this parameter is automatically reset to Power Up in Operational Mode. When the module senses no Ethernet link within 15 minutes after power up, the SM carrier shuts off.
- **Power Up in Operational Mode**—the SM boots in Operational mode. The module attempts registration. This is the default selection.

Bridge Entry Timeout

Specify the appropriate bridge timeout for correct network operation with the existing network infrastructure. Timeout occurs when the AP encounters no activity with the SM

(whose MAC address is the bridge entry) within the interval that this parameter specifies. The Bridge Entry Timeout should be a longer period than the ARP (Address Resolution Protocol) cache timeout of the router that feeds the network.

This parameter governs the timeout interval, even if a router in the system has a longer timeout interval. The default value of this field is 25 minutes.

CAUTION!
An inappropriately low Bridge Entry Timeout setting may lead to temporary loss of communication with some end users.

Authentication Key

Only if the AP to which this SM will register requires authentication, specify the key that the SM should use when authenticating:

- **Use Default Key** specifies the predetermined key for authentication in the BAM server. See Authentication Manager Capability on Page 307.
- **Use This Key** specifies the 32-digit hexadecimal key that is permanently stored on both the SM and the BAM database.

NOTE:
In Release 4.2.2 and earlier releases, if you enter the same key but as fewer than 32 digits in the SM and BAM database, the SM cannot authenticate despite the match. In Release 4.2.3 and later releases, the SM and BAM server pad the key of any length by the addition of leading zeroes, and if the entered keys match, authentication attempts succeed. However, Canopy recommends that you enter 32 characters to achieve the maximal security from this feature.

Frame Timing Pulse Gated

If this SM extends the sync pulse to a BH master or an AP, select either

- **Enable**—If this SM loses sync from the AP, then *do not* propagate a sync pulse to the BH timing master or other AP. This setting prevents interference in the event that the SM loses sync.
- **Disable**—If this SM loses sync from the AP, then propagate the sync pulse to the BH timing master or other AP.

See Wiring to Extend Network Sync on Page 294.

Power Control

In Release 4.1 and later releases, select either

- **Low** to set the SM to operate at 18 dB less than full power to reduce the possibility of self-interference with a nearby module.
- **Normal** to allow the SM to operate at full power.

CAUTION!

Selection of **Low** can cause the SM to drop an active RF link to an AP that is relatively far from the low-power SM. If a link is dropped when Power Control is set to **Low**, the link can be re-established by only Ethernet access.

If you select **Low** and save the changes and reboot the AP, you should immediately open the Link Test page and perform a link test.

Community String

Specify a control string that allows a NMS (Network Management Station) to access MIB information about this SM. No spaces are allowed in this string. The default string is **Canopy**.

The **Community String** value is clear text and is readable by a packet monitor. Additional security derives from the configuration of the **Accessing Subnet**, **Trap Address**, and **Permission** parameters.

Accessing Subnet

Specify the addresses that are allowed to send SNMP requests to this SM. The NMS has an address that is among these addresses (this subnet). You must enter both

- The network IP address in the form xxx.xxx.xxx.xxx
- The CIDR (Classless Interdomain Routing) prefix length in the form /xx

For example

- the /16 in 198.32.0.0/16 specifies a subnet mask of 255.255.0.0 (the first 16 bits in the address range are identical among all members of the subnet).
- 192.168.102.0 specifies that any device whose IP address is in the range 192.168.102.0 to 192.168.102.254 can send SNMP requests to the SM, presuming that the device supplies the correct **Community String** value.

The default treatment is to allow all networks access (set to 0). For more information on CIDR, execute an Internet search on “Classless Interdomain Routing.”

RECOMMENDATION:
The subscriber can access the SM by changing the subscriber device to the accessing subnet. This hazard exists because the **Community String** and **Accessing Subnet** are both visible parameters. To avoid this hazard in Release 4.2 or a later release, configure the SM to filter (block) SNMP requests. See Filtering Protocols and Ports on Page 303.

Trap Address

Specify the IP address (xxx.xxx.xxx.xxx) of an NMS to which trap information should be sent. Trap information informs the NMS that something has occurred. For example, trap information is sent:

- after a reboot of the module.
- when an NMS attempts to access agent information but either
  - supplied an inappropriate community string or SNMP version number.
  - is associated with a subnet to which access is disallowed.

Permission

Select **Read Only** if you wish to disallow any parameter changes by the NMS.

Site Name

Specify a string to associate with the physical module. This parameter is written into the *sysName* SNMP MIB-II object and can be polled by an NMS. The buffer size for this field is 128 characters.

Site Contact

Enter contact information for the module administrator. This parameter is written into the *sysContact* SNMP MIB-II object and can be polled by an NMS. The buffer size for this field is 128 characters.

Site Location

Enter information about the physical location of the module. This parameter is written into the *sysLocation* SNMP MIB-II object and can be polled by an NMS. The buffer size for this field is 128 characters.

The Configuration page also provides the following buttons.

Save Changes

When you click this button, any changes that you made on the Configuration page are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Undo Saved Changes

When you click this button, any changes that you made but were not committed by a reboot of the module are undone.

Set to Factory Defaults

When you click this button, *all configurable parameters on all configurable pages* are reset to the factory settings.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

Whenever you change a parameter in the Configuration page, the system highlights the **Reboot** button as a reminder that a reboot (in addition to a save) is required to implement the changes.

18.2.2 IP Configuration Page of the SM with NAT Disabled

Examples of SM IP Configuration screens are displayed in

- Figure 77 for the NAT Disabled implementation with public accessibility.
- Figure 78 for the NAT Disabled implementation with local accessibility.

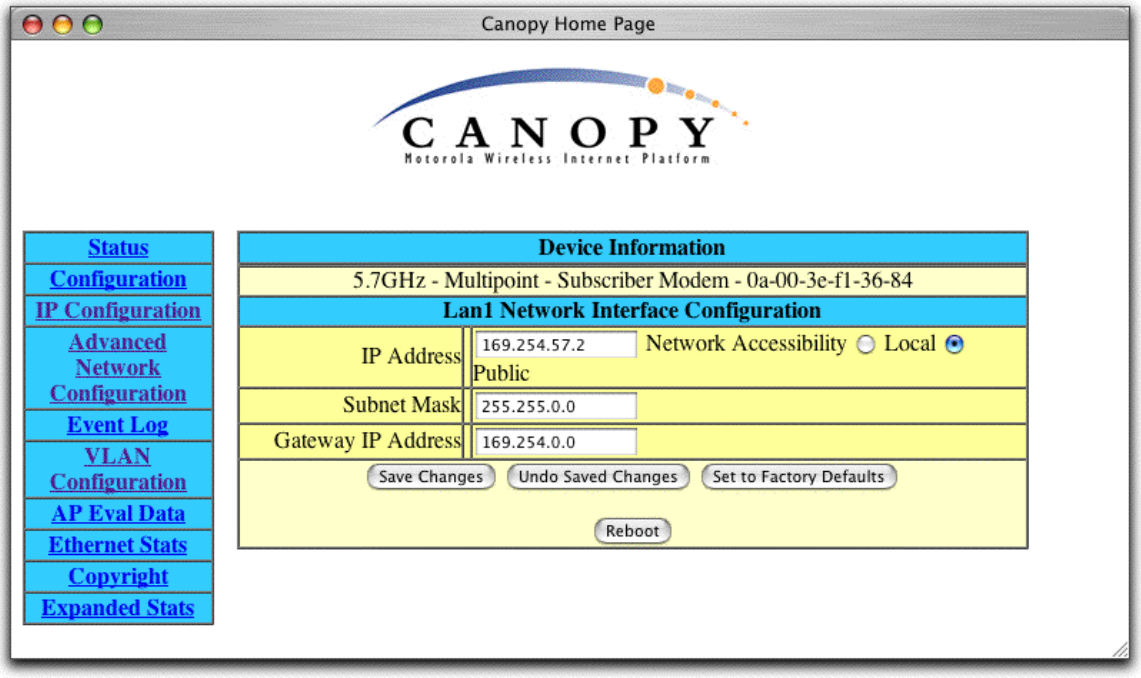


Figure 77: IP Configuration screen, NAT disabled, public accessibility

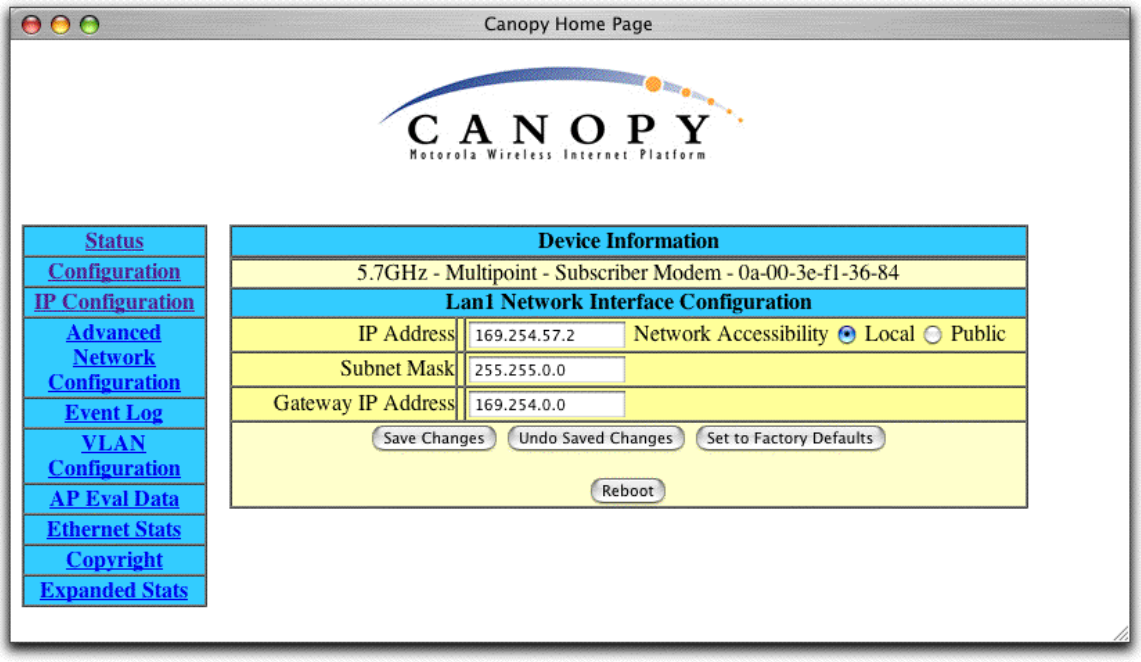


Figure 78: IP Configuration screen, NAT disabled, local accessibility

When NAT (network address translation) is disabled on the NAT Configuration page as shown in Figure 83 on Page 223, the you may set the following IP Configuration page parameters.

LAN1 Network Interface Configuration, IP Address

Enter the *non-routable* IP address to associate with the Ethernet connection on this SM. (The default IP address from the factory is 169.254.1.1.) If you set and then forget this parameter, then you must both

1. physically access the module.
2. use an override plug to electronically access the module configuration parameters at 169.254.1.1. See Overriding Forgotten IP Addresses or Passwords on AP, SM, or BH on Page 302.

RECOMMENDATION:
Note or print the IP settings from this page. Ensure that you can readily associate these IP settings both with the module and with the other data that you store about the module.

LAN1 Network Interface Configuration, Subnet Mask

Enter an appropriate subnet mask for the SM to communicate on the network. The default subnet mask is 255.255.255.0. See Allocating Subnets on Page 123.

LAN1 Network Interface Configuration, Gateway IP Address

Enter the appropriate gateway for the SM to communicate with the network. The default gateway is 169.254.0.0.

Regardless of whether NAT is enabled, the IP Configuration page also provides the following buttons.

Save Changes

When you click this button, any changes that you made on the IP Configuration page are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Undo Saved Changes

When you click this button, any changes that you made but were not committed by a reboot of the module are undone.

Set to Factory Defaults

When you click this button, *all configurable parameters on all configurable pages* are reset to the factory settings.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

Whenever you change a parameter in the IP Configuration page, the system highlights the **Reboot** button as a reminder that a reboot (in addition to a save) is required to implement the changes.

18.2.3 IP Configuration Page of the SM with NAT Enabled

Further examples of SM IP Configuration screens are displayed in

- Figure 79 for the NAT with DHCP Client and DHCP Server implementation.
- Figure 80 for the NAT with DHCP Client implementation.
- Figure 81 for the NAT with DHCP Server implementation.
- Figure 82 for the NAT without DHCP implementation.

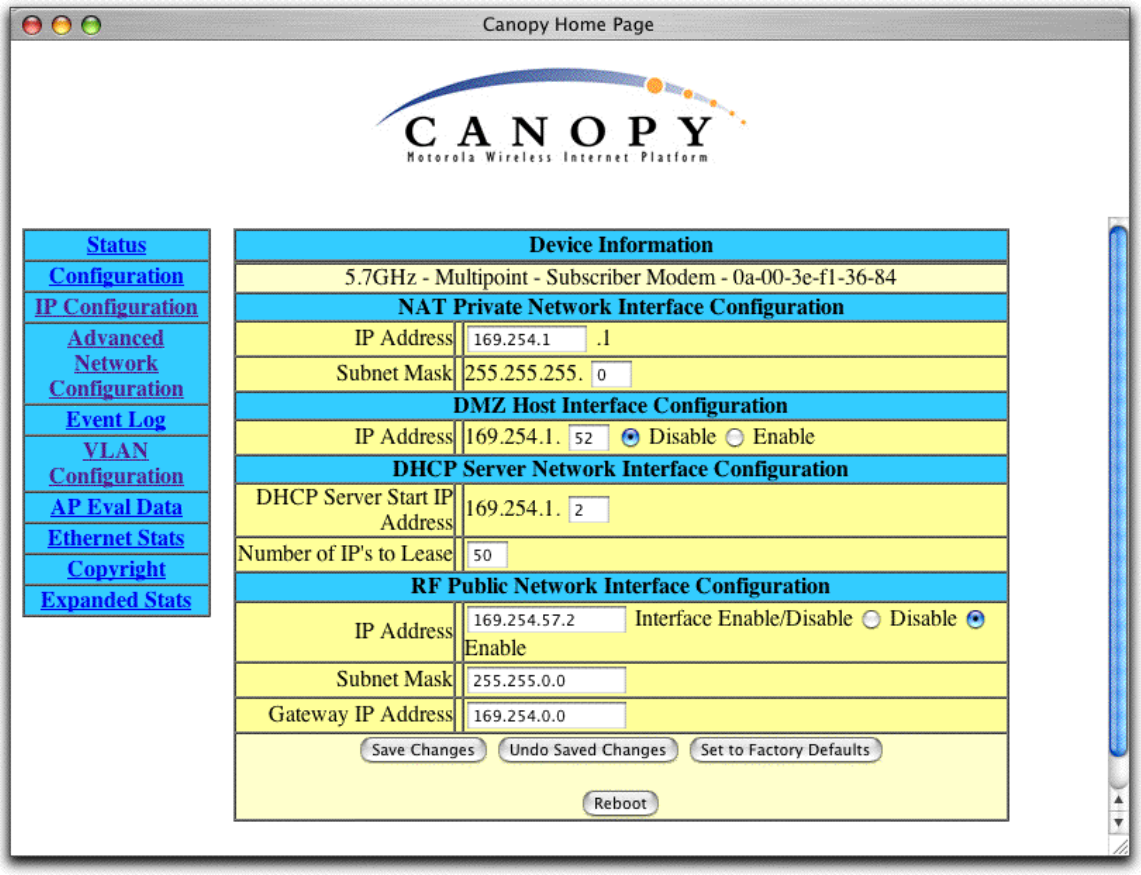


Figure 79: IP Configuration screen, NAT with DHCP client and DHCP server

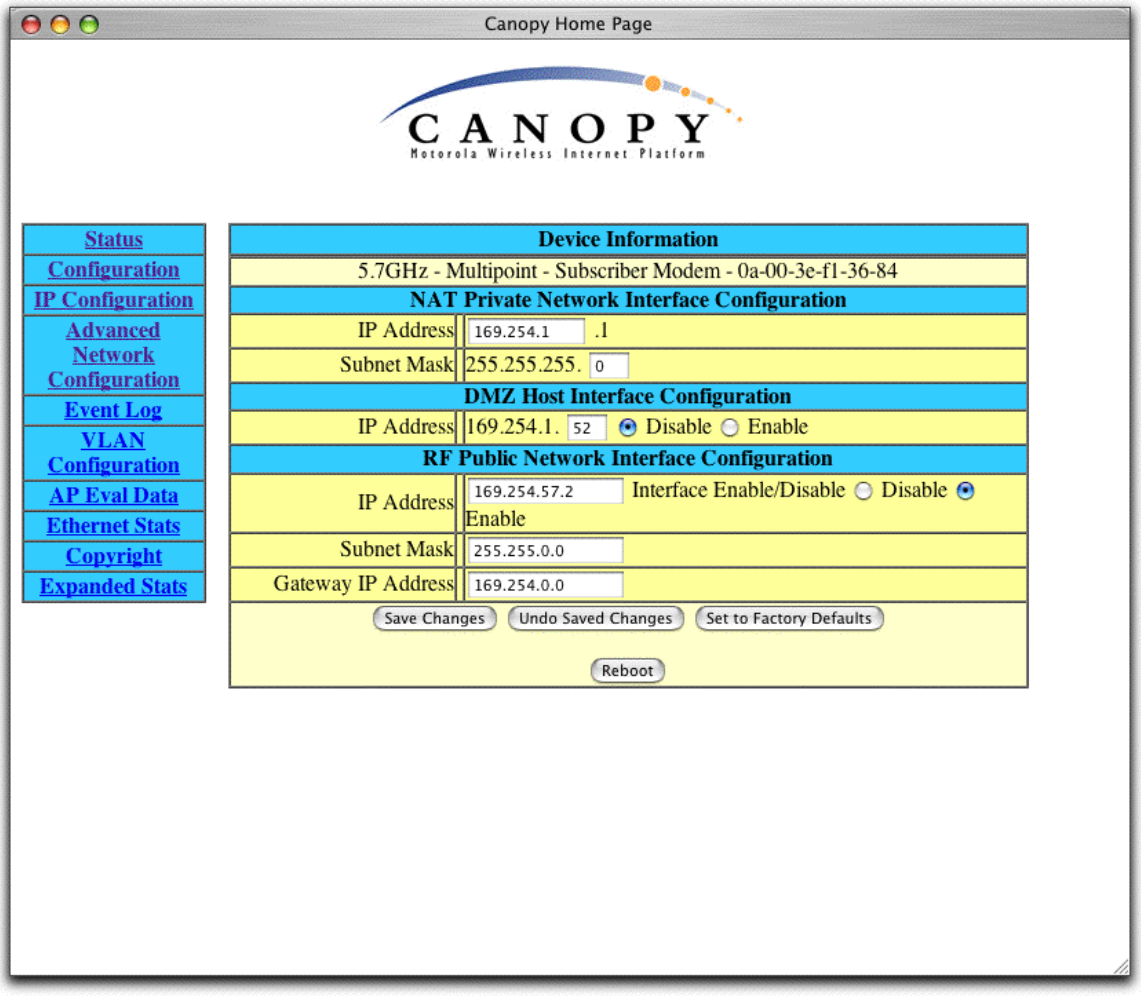


Figure 80: IP Configuration screen, NAT with DHCP client

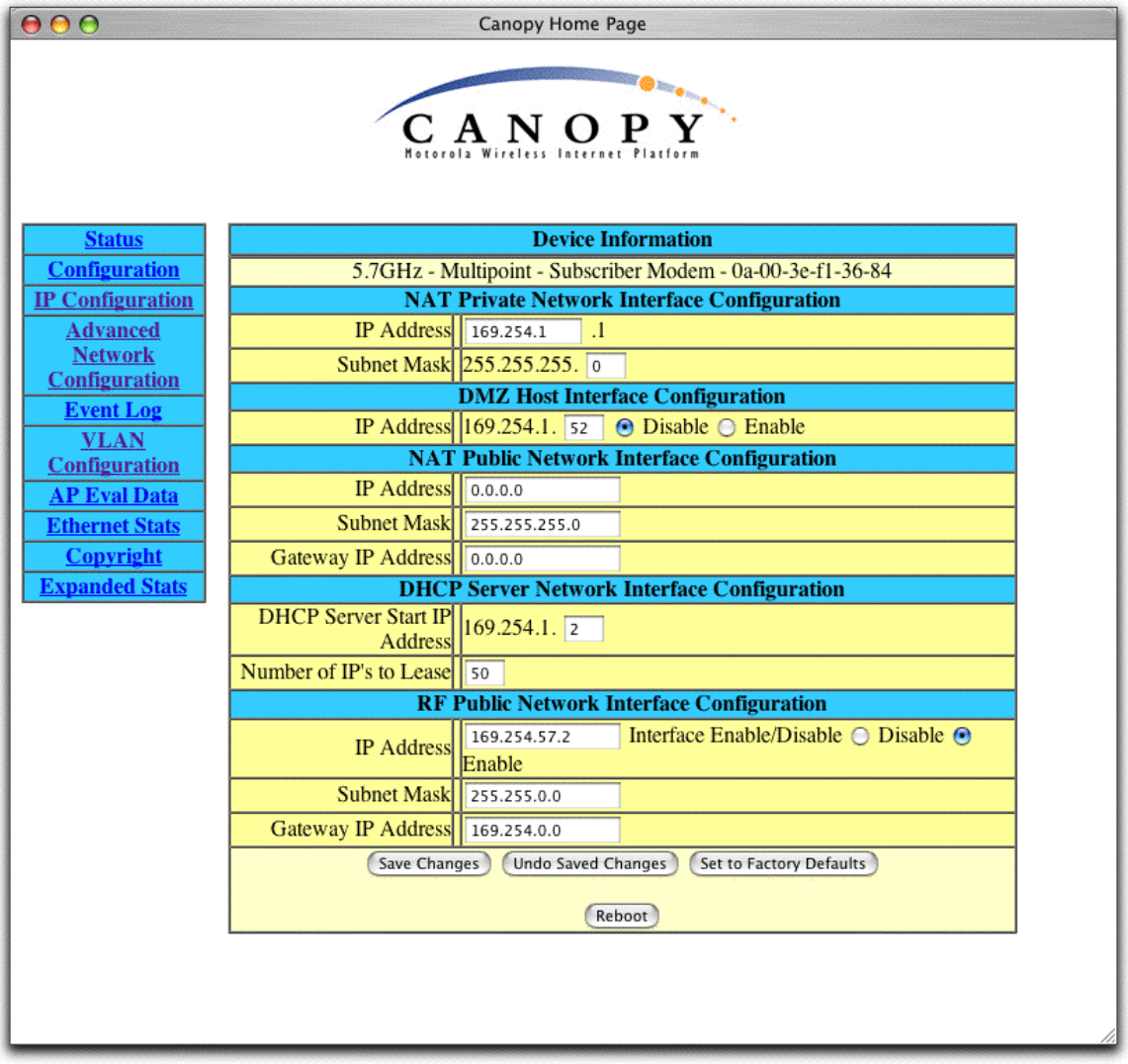


Figure 81: IP Configuration screen, NAT with DHCP server

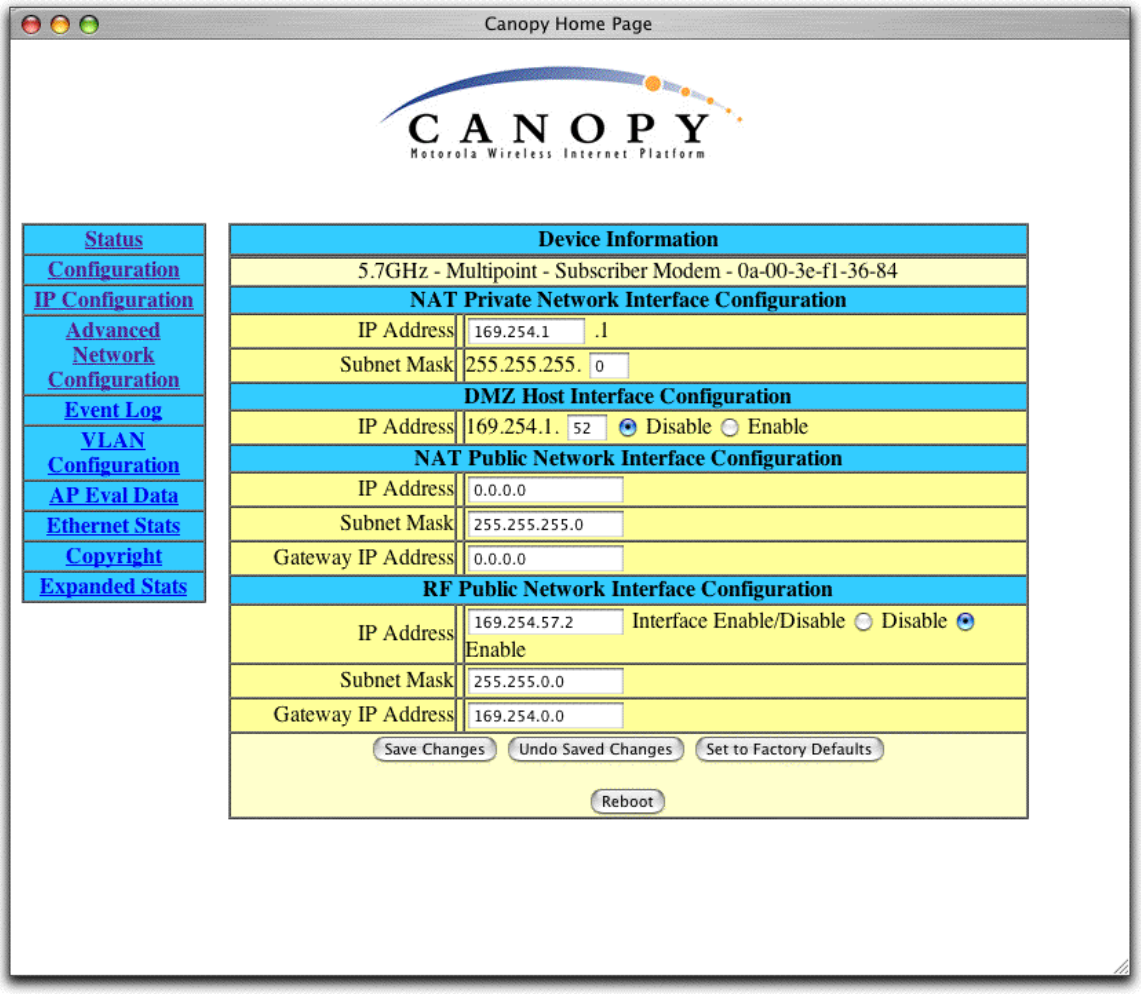


Figure 82: IP Configuration screen, NAT without DHCP

When NAT (network address translation) is enabled, you may set the following IP Configuration page parameters.

NAT Private Network Interface Configuration, IP Address

Assign an IP address for SM management. This address is available from only Ethernet access to the SM. The last characters of this address must be .1. This address becomes the base for the range of DHCP-assigned addresses.

NAT Private Network Interface Configuration, Subnet Mask

Assign a subnet mask of 255.255.255.0 or a more restrictive subnet mask.

DMZ Host Interface Configuration, IP Address

Either enable or disable DMZ for this SM. See DMZ on Page 117.

Also assign the DMZ IP address to use for this SM when DMZ is enabled. The first three octets of this address are automatically set as identical to the first three octets of the

address assigned in the **NAT Private Network Interface Configuration, IP Address** field above. Only one such address is allowed.

Behind this SM, the device that should receive network traffic must be assigned this address. The system provides a warning if you enter an address within the range that DHCP can assign.

NAT Public Network Interface Configuration, IP Address

This field displays the IP address of the SM. If DHCP Client is enabled, then the DHCP server automatically assigns this address.

NAT Public Network Interface Configuration, Subnet Mask

This field displays the subnet mask of the SM. If DHCP Client is enabled, then the DHCP server automatically assigns this subnet mask.

NAT Public Network Interface Configuration, Gateway IP Address

This field displays the gateway IP address for the SM. If DHCP Client is enabled, then the DHCP server automatically assigns this gateway IP address.

RF Public Network Interface Configuration, IP Address

Either enable or disable the RF public interface for this SM. Also assign the IP address for over-the-air management of the SM when the RF public interface is enabled.

RF Public Network Interface Configuration, Subnet Mask

Assigns the subnet mask for over-the-air management of the SM when the RF public interface is enabled.

RF Public Network Interface Configuration, Gateway IP Address

Assigns the gateway IP address for over-the-air management of the SM when the RF public interface is enabled.

RECOMMENDATION:
Note or print the IP settings from this page. Ensure that you can readily associate these IP settings both with the module and with the other data that you store about the module.

Regardless of whether NAT is enabled, the IP Configuration page also provides the following buttons.

Save Changes

When you click this button, any changes that you made on the IP Configuration page are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Undo Saved Changes

When you click this button, any changes that you made but were not committed by a reboot of the module are undone.

Set to Factory Defaults

When you click this button, *all configurable parameters on all configurable pages* are reset to the factory settings.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

Whenever you change a parameter in the IP Configuration page, the system highlights the **Reboot** button as a reminder that a reboot (in addition to a save) is required to implement the changes.

18.2.4 NAT Configuration Page of the SM with NAT Disabled

An example of the SM NAT Configuration page when NAT (network address translation) is disabled is shown in Figure 83. The default state of the SM is with NAT disabled.

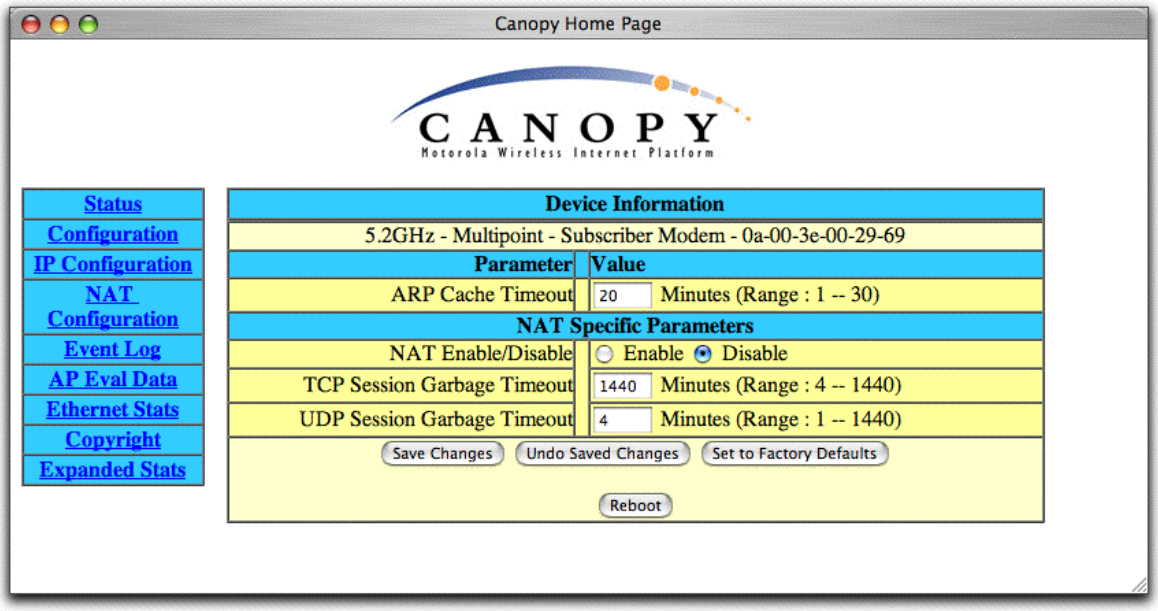


Figure 83: NAT Configuration screen, NAT disabled

When NAT (network address translation) is disabled, you may set the following NAT Configuration page parameters.

ARP Cache Timeout

If a router upstream has an ARP cache of longer duration (as some use 30 minutes), enter a value of longer duration than the router ARP cache. The default value of this field is 20 seconds.

NAT Enable/Disable

Either disable NAT, or enable NAT to view additional options.

TCP Session Garbage Timeout

Where a large network exists behind the SM, you can set this parameter to lower than the default value of 1440 minutes (24 hours). This action makes additional resources available for greater traffic than the default value accommodates.

UDP Session Garbage Timeout

You may adjust this parameter in the range of 1 to 1440 minutes, based on network performance. The default value of this parameter is 4 minutes.

Regardless of whether NAT is enabled, the NAT Configuration page also provides the following buttons.

Save Changes

When you click this button, any changes that you made on the NAT Configuration page are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Undo Saved Changes

When you click this button, any changes that you made but were not committed by a reboot of the module are undone.

Set to Factory Defaults

When you click this button, *all configurable parameters on all configurable pages* are reset to the factory settings.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

Whenever you change a parameter in the NAT Configuration page, the system highlights the **Reboot** button as a reminder that a reboot (in addition to a save) is required to implement the changes.

18.2.5 Advanced Network Configuration Page of the SM with NAT Disabled

An example of the SM Advanced Network Configuration page when NAT (network address translation) is disabled is shown in Figure 84. The default state of this page is with NAT disabled.

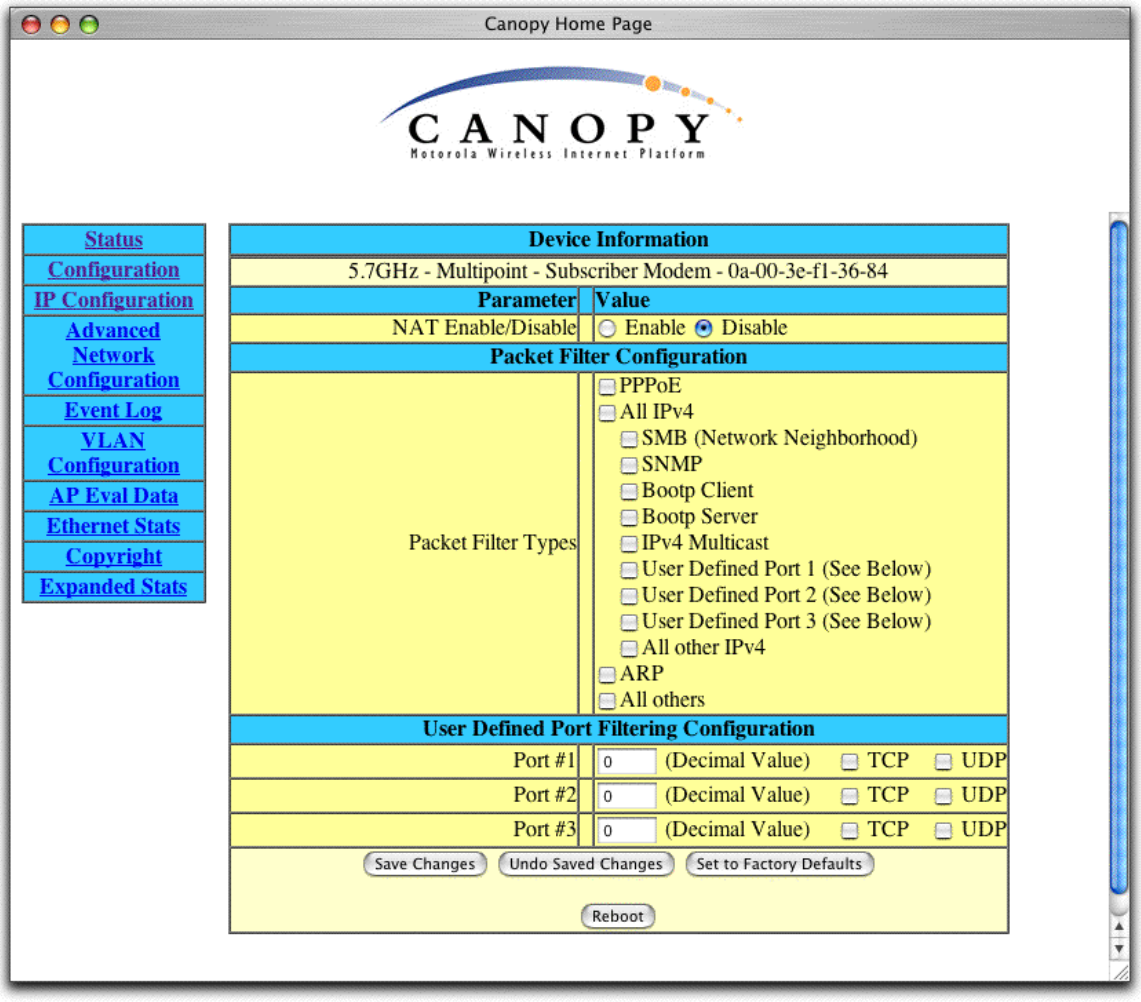


Figure 84: Advanced Network Configuration screen of SM with NAT disabled

When NAT (network address translation) is disabled, you may set the following Advanced Network Configuration page parameters.

NAT Enable/Disable

Either disable NAT, or enable NAT to view additional options.

Packet Filter Configuration

In Release 4.2 and later releases, for any box selected, the Protocol and Port Filtering feature blocks the associated protocol type. Examples are provided in Protocol and Port Filtering with NAT Disabled on Page 303.

User Defined Port Filtering Configuration

In Release 4.2 and later releases, you can specify ports for which to block subscriber access, regardless of whether NAT is enabled. See Filtering Protocols and Port on Page 303.

Save Changes

When you click this button, any changes that you made on the NAT Configuration page are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Undo Saved Changes

When you click this button, any changes that you made but were not committed by a reboot of the module are undone.

Set to Factory Defaults

When you click this button, *all configurable parameters on all configurable pages* are reset to the factory settings.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

Whenever you change a parameter in the NAT Configuration page, the system highlights the **Reboot** button as a reminder that a reboot (in addition to a save) is required to implement the changes.

18.2.6 NAT/Advanced Network Configuration Page of the SM with NAT Enabled

Examples of SM NAT Configuration screens when NAT is enabled are displayed in

- Figure 85 for the NAT with DHCP Client and DHCP Server implementation.
- Figure 86 for the NAT with DHCP Client implementation.
- Figure 87 for the NAT with DHCP Server implementation.
- Figure 88 for the NAT without DHCP implementation.

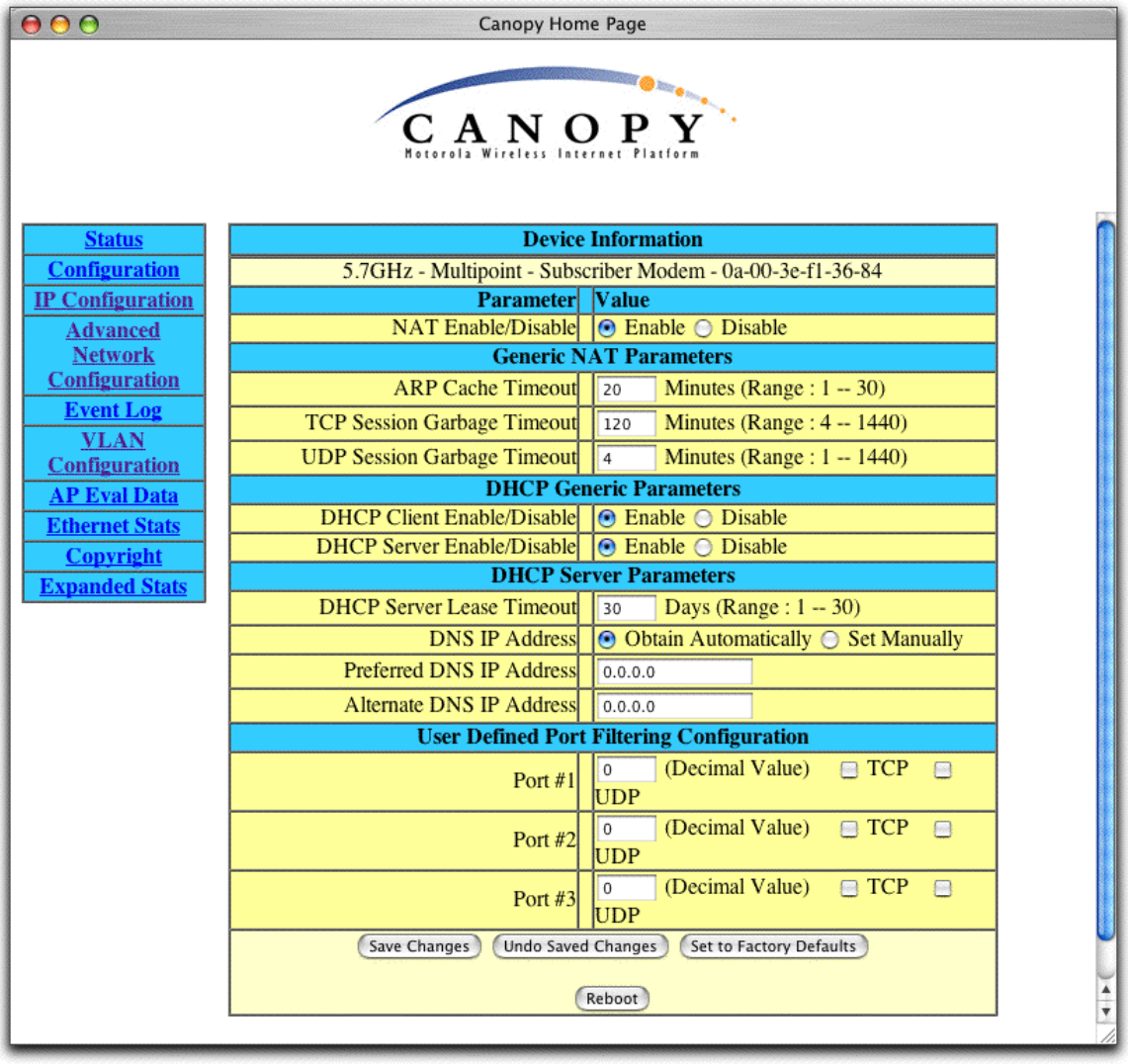


Figure 85: Advanced Network Configuration screen, NAT with DHCP client and DHCP server

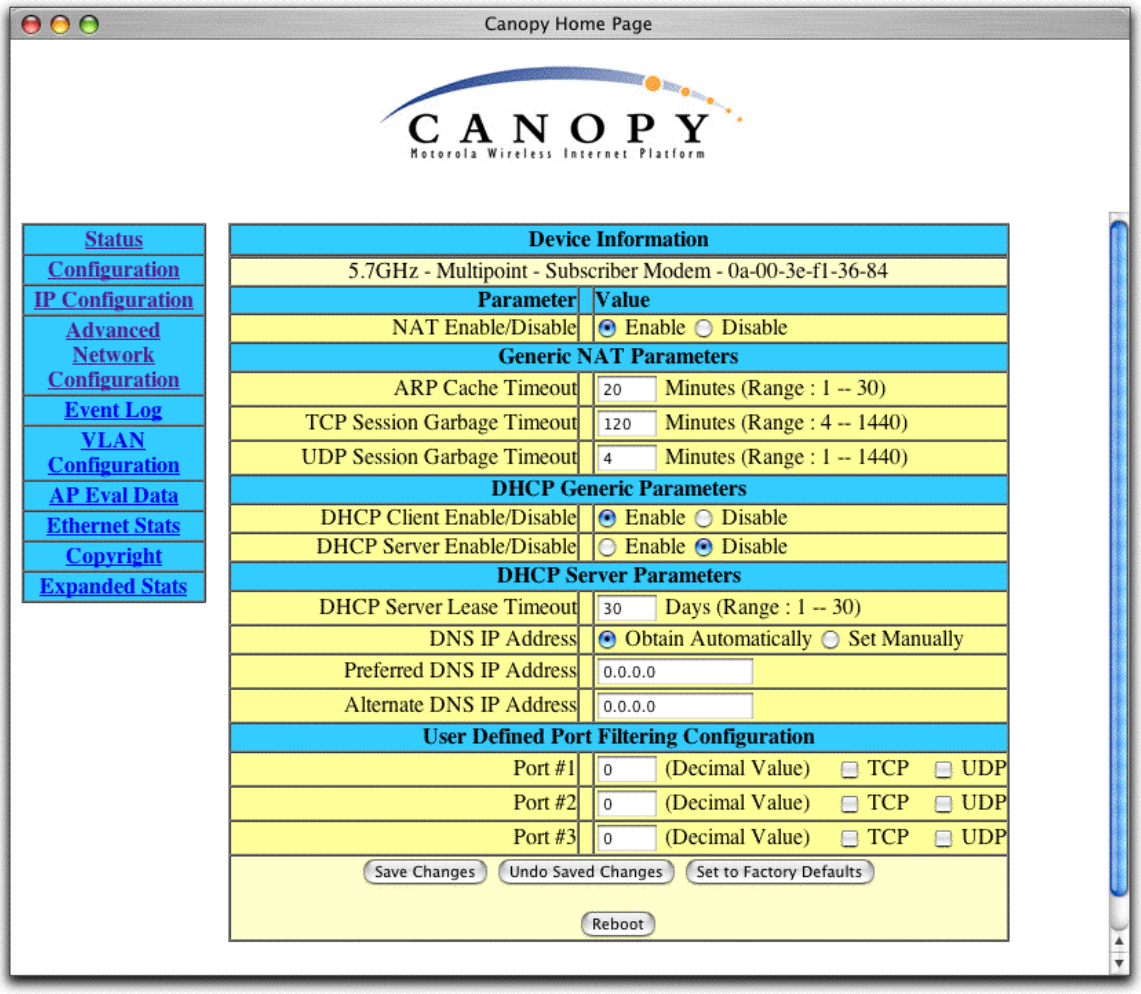


Figure 86: NAT Configuration screen, NAT with DHCP client

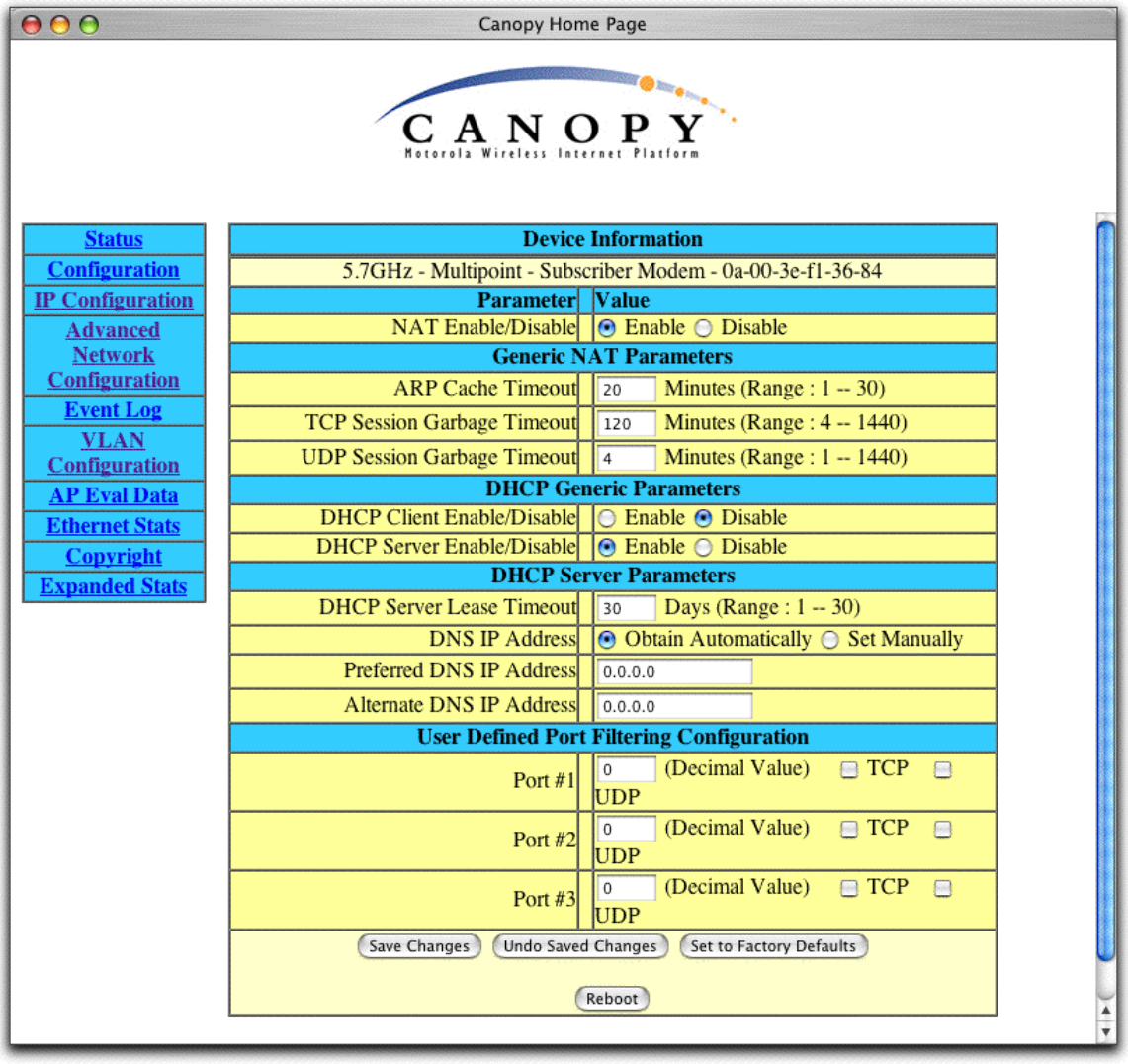


Figure 87: NAT Configuration screen, NAT with DHCP server

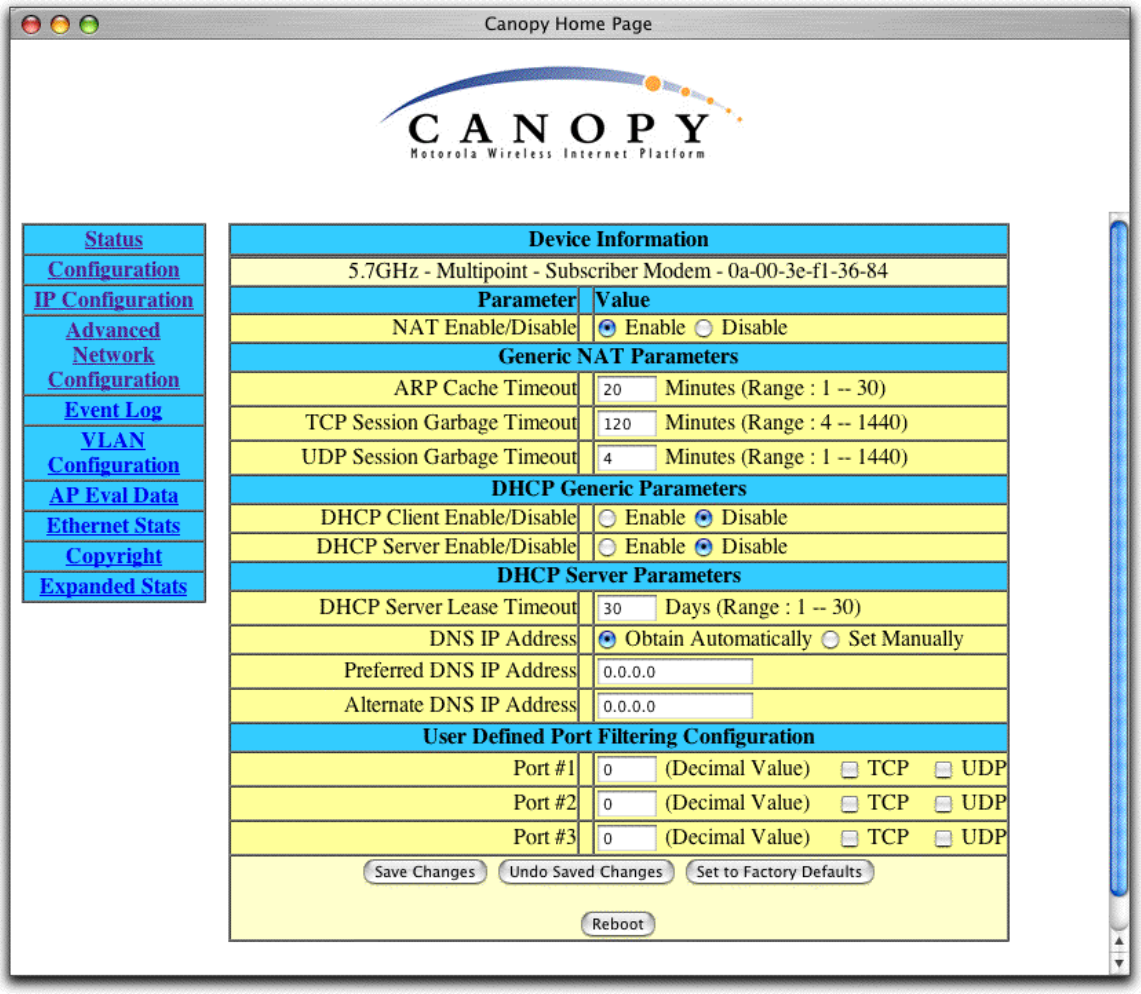


Figure 88: NAT Configuration screen, NAT without DHCP

When NAT (network address translation) is enabled, you may set the following NAT Configuration page parameters.

ARP Cache Timeout

If a router upstream has an ARP cache of longer duration (as some use 30 minutes), enter a value of longer duration than the router ARP cache. The default value of this field is 20 seconds.

NAT Enable/Disable

Either disable NAT, or enable NAT to view additional options.

TCP Session Garbage Timeout

Where a large network exists behind the SM, you can set this value to lower than the default value of 1440 minutes (24 hours). This action makes additional resources available for greater traffic than the default value accommodates.

UDP Session Garbage Timeout

You may adjust this value in the range of 1 to 1440 minutes, based on network performance. The default value of this parameter is 4 minutes.

DHCP Client Enable/Disable

Select either

- **Enable** to allow the network DHCP server to assign the NAT Public Network Interface Configuration IP address, subnet mask, and gateway IP address for this SM.
- **Disable** to
  - disable DHCP server assignment of this address.
  - enable the operator to assign this address.

DHCP Server Enable/Disable

Select either

- **Enable** to
  - allow this SM to assign IP addresses, subnet masks, and gateway IP addresses to attached devices.
  - assign a start address for the SM.
  - designate how many IP addresses may be leased on the IP Configuration page of this SM.
- **Disable** to disallow the SM to assign addresses to attached devices.

DHCP Server Lease Timeout

You may adjust this parameter in the range of 1 to 30 days, based on network performance. The default value of this parameter is 30 days.

DNS IP Address

Select either

- **Obtain Automatically** to allow the system to set the IP address of the DNS server.
- **Set Manually** to enable yourself to set both a preferred and an alternate DNS IP address.

Preferred DNS IP Address

If the **DNS IP Address** parameter is set to **Set Manually**, set this parameter as the preferred address of the DNS server.

Alternate DNS IP Address

If the **DNS IP Address** parameter is set to **Set Manually**, set this parameter as the alternate address of the DNS server.

User Defined Port Filtering Configuration

This parameter is shown in Figure 85 on Page 227. In Release 4.2 and later releases, you can specify ports for which to block subscriber access, regardless of whether NAT is enabled. See Filtering Protocols and Port on Page 303.

18.2.7 NAT Configuration Buttons with NAT Enabled

Regardless of whether NAT is enabled, the NAT Configuration page also provides the following buttons.

Save Changes

When you click this button, any changes that you made on the NAT Configuration page are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Undo Saved Changes

When you click this button, any changes that you made but were not committed by a reboot of the module are undone.

Set to Factory Defaults

When you click this button, *all configurable parameters on all configurable pages* are reset to the factory settings.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

Whenever you change a parameter in the NAT Configuration page, the system highlights the **Reboot** button as a reminder that a reboot (in addition to a save) is required to implement the changes.

18.2.8 VLAN Configuration Page of the SM

An example screen of the VLAN Configuration page of the SM is displayed in FGR.

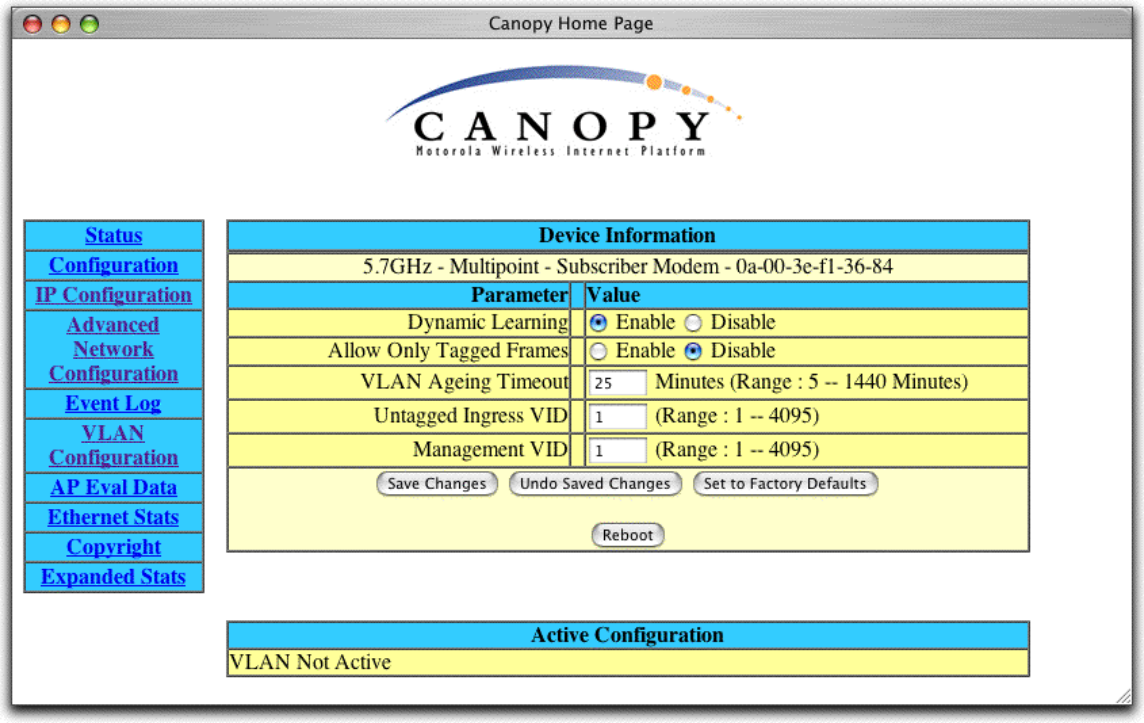


Figure 89: VLAN Configuration screen, SM

You may set the VLAN Configuration page parameters as follows.

Dynamic Learning

Specify whether the SM should (**Enable**) or should not (**Disable**) add the VIDs of upstream frames (that enter the SM through the wired Ethernet interface) to the VID table. The default value is **Enable**.

Allow Only Tagged Frames

Specify whether the SM should drop (**Enable**) frames that arrive without a tag at its wired Ethernet interface or should tag (**Disable**) those untagged frames using the VID that is stored in the **Untagged Ingress VID** parameter. The default value is **Disable**.

VLAN Aging Timeout

Specify how long the SM should keep dynamically learned VIDs. The range of values is 5 to 1440 (minutes). The default value is **25** (minutes).

NOTE:
VIDs that you enter for the **Untagged Ingress VID** and **Management VID** parameters do not time out.

Untagged Ingress VID

Enter the VID that the SM should use to tag frames that arrive untagged at its wired Ethernet interface. The range of values is 1 to 4095. The default value is **1**.

Management VID

Enter the VID that the SM should share with the AP. The range of values is 1 to 4095. The default value is **1**.

18.3 SETTING THE CONFIGURATION SOURCE

In Canopy System Release 6.1 and later releases, the AP includes a **Configuration Source** parameter, which sets where SMs that register to the AP are controlled for MIR, VLAN, the high-priority channel, and CIR as follows.

In a sector where **Software Scheduling** is implemented, the **Configuration Source** parameter affects the source of

- all MIR settings:
  - **Sustained Uplink Data Rate**
  - **Uplink Burst Allocation**
  - **Sustained Downlink Data Rate**
  - **Downlink Burst Allocation**
- all SM VLAN settings:
  - **Dynamic Learning**
  - **Allow Only Tagged Frames**
  - **VLAN Aging Timeout**
  - **Untagged Ingress VID**
  - **Management VID**
  - **VLAN Membership**

In a sector where **Hardware Scheduling** is implemented, the **Configuration Source** parameter affects the source of

- all MIR settings:
  - **Sustained Uplink Data Rate**
  - **Uplink Burst Allocation**
  - **Sustained Downlink Data Rate**
  - **Downlink Burst Allocation**
- all SM VLAN settings:
  - **Dynamic Learning**
  - **Allow Only Tagged Frames**
  - **VLAN Aging Timeout**
  - **Untagged Ingress VID**
  - **Management VID**
  - **VLAN Membership**
- the **Hi Priority Channel** setting
- all CIR settings
  - **Low Priority Uplink CIR**
  - **Low Priority Downlink CIR**

- **Hi Priority Uplink CIR**
- **Hi Priority Downlink CIR**

For any SM whose **Authentication Mode** parameter is set to **Authentication Required**, the above settings are derived as shown in Table 42.

Table 42: Where feature values are obtained for the SM with authentication required

Configuration Source Setting in the AP	Where These Values are Obtained in a Sector with							
	Software Scheduling				Hardware Scheduling			
	All MIR	All VLAN	HPC	All CIR	All MIR	All VLAN	HPC	All CIR
BAM	BAM	BAM	AP	n/a	BAM	BAM	BAM	BAM
SM	SM	SM	AP	n/a	SM	SM	SM	SM

NOTES:

HPC represents the **Hi Priority Channel** (enable or disable).

CIR is not available to SMs in a sector where Software Scheduling is implemented.

Where *BAM* is the indication, values in the SM are disregarded.

Where *SM* is the indication, values that BAM sends for the SM are disregarded.

The high-priority channel is unavailable to older SMs that have Hardware Scheduling enabled.

Table 43: Where feature values are obtained for the SM with authentication disabled

Configuration Source Setting in the AP	Where These Values are Obtained in a Sector with							
	Software Scheduling				Hardware Scheduling			
	All MIR	All VLAN	HPC	All CIR	All MIR	All VLAN	HPC	All CIR
BAM	AP	AP	AP	n/a	AP	AP	AP	AP
SM	SM	SM	AP	n/a	SM	SM	SM	SM

18.4 CONFIGURING A BH TIMING MASTER FOR THE DESTINATION

NOTE:
The 45-Mbps BH is described in the dedicated document *Canopy 45-Mbps Backhaul User Guide*.

18.4.1 Configuration Page of the BHM

An example of a BHM Configuration screen is displayed in Figure 90.

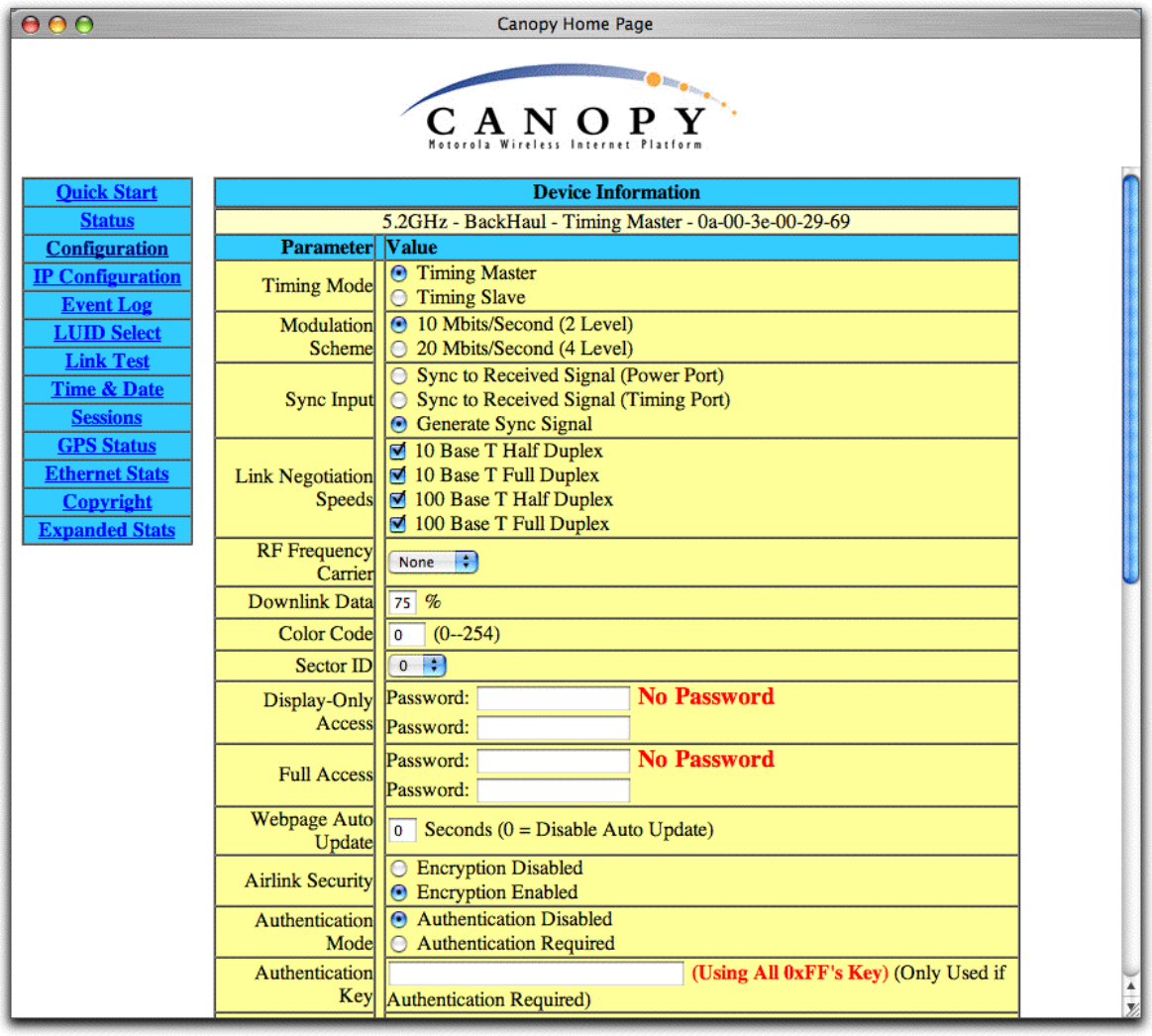


Figure 90: Configuration screen, BHM

The Configuration web page contains all of the configurable parameters that define how the module operates. The first line of information on the Configuration screen echoes the **Device Type** from the Status web page.

You may set the Configuration page parameters as follows.

Device Information

This parameter indicates the frequency band of the module, whether this BH serves as timing master or timing slave, and the MAC address of the module.

Timing Mode

Select **Timing Master**. This BH will provide sync for the link. Whenever you toggle this parameter to Timing Master from Timing Slave, you should also do the following:

1. Make no other changes in this or any other interface page.
2. Save this change of timing mode.
3. Reboot the BH.

RESULT: The set of interface web pages that is unique to a BHM is made available.

Modulation Scheme

This parameter is available for only the 20-Mbps BH. You can specify in this parameter whether to use this 20-Mbps BH as a 10-Mbps BH.

Sync Input

Specify the type of synchronization for this BH timing master to use.

- Select **Sync to Received Signal (Power Port)** to set this BHM to receive sync from a connected CMMmicro.
- Select **Sync to Received Signal (Timing Port)** to set this BHM to receive sync from a connected CMM2, an AP in the cluster, an SM, or a BH timing slave.
- Select **Generate Sync Signal** where the BHM does not receive sync, and no AP or other BHM is active within the link range. For link range information, see Table 28 on Page 111.

Link Negotiation Speeds

Specify the type of link speed for the Ethernet connection. The default for this parameter is that all speeds are selected. The recommended setting is a single speed selection for all APs, BHs, and SMs in the operator network.

RF Frequency Carrier

Specify the frequency for the BHM to transmit. The default for this parameter is **None**. (The selection labeled **Factory** requires a special software key file for implementation.) In a 5.7-GHz BHM, this parameter displays both ISM and U-NII frequencies. In a 5.2-GHz BHM, this parameter displays only ISM frequencies. For a list of channels in the band, see Considering Frequency Band Alternatives on Page 100.

Downlink Data

The operator specifies the percentage of the aggregate throughput that is needed for the downlink. For example, if the aggregate (uplink and downlink total) throughput on the module is 6 Mb, then 75% specified for this parameter allocates 4.5 Mb for the downlink and 1.5 Mb for the uplink. The default for this parameter is 75%.

Color Code

Specify a value from 0 to 254. For registration to occur, the color code of the BHS and the BHM *must* match. Color code is not a security feature. Instead, color code allows you to segregate an individual network or neighboring Canopy networks.

Color code also allows you to force an BHS to register to only a specific BHM, even where the BHS can reach multiple BHMs. On all Canopy modules, the default setting for the color code value is 0. This value matches only the color code of 0 (*not* all 255 color codes).

RECOMMENDATION:
Note the color code that you enter. Ensure that you can readily associate this color code both with the module and with the other data that you store about the module.

Sector ID

Specify a number to associate with this BHM. The Sector ID does not affect the operation of the BHM. On the AP Eval Data web page of the BHS, the **Sector ID** field identifies the BHM that the BHS sees. For efficient and accurate network management, you should

- assign a unique Sector ID to each sector.
- repeat the assignment pattern throughout the entire Canopy system.

Display-Only Access

If you set (populate) the **Display-Only Access** password, this password will allow only *viewing* activities on the module.

This protection interacts with the **Full Access** password protection as follows:

- If the **Display-Only Access** password is set and the **Full Access** password *is not*, then the **Display-Only Access** password allows
  - telnet and FTP access to the module.
  - *viewing or changing* the parameters of the module. This configuration *is not* recommended.
- If the **Full Access** password is also set, then the **Full Access** password allows telnet and FTP access to the module, and the **Display-Only Access** password does not.
- If the **Display-Only Access** password *is not* set and the **Full Access** password is, then no password is required to view the parameters of the module.
- If neither password is set, then anyone can *view or change* the parameters of the module. This configuration *is not* recommended.

To set this password, enter the same expression in both **Display-Only Access** fields for verification. When the web-based interface prompts for this password, no user name is required. However, when a telnet or FTP session prompts for this password, you must enter the user name `root` in addition to the password.

If you set and then forget the **Display-Only Access** password, then you must both

1. physically access the module.
2. use an override plug to electronically access the module configuration parameters at 169.254.1.1. See Overriding Forgotten IP Addresses or Passwords on AP, SM, or BH on Page 302.

Full Access

If you set the **Full Access** password, this password will allow

- telnet and FTP access to the module.
- *viewing or changing* the parameters of the module.

To set this password, enter the same expression in both **Full Access** fields for verification. When the web-based interface prompts for this password, no user name is required. However, when a telnet or FTP session prompts for this password, you must enter the user name `root` in addition to the password.

If you set and then forget the **Full Access** password, then you must both

1. physically access the module.
2. use an override plug to electronically access the module configuration parameters at 169.254.1.1. See Overriding Forgotten IP Addresses or Passwords on AP, SM, or BH on Page 302.

NOTE:
You can unset either password (revert the access to no password required). To do so, type a space into the field and reboot the module. You must enter any password twice to allow the system to verify that the password is not mistyped. After any password is set and a reboot of the module has occurred, a **Password Set** indicator appears to the right of the field.

RECOMMENDATION:
Note the passwords that you enter. Ensure that you can readily associate these passwords both with the module and with the other data that you store about the module.

Webpage Auto Update

Enter the frequency (in seconds) for the web browser to automatically refresh the web-based interface. The default setting is 0. The 0 setting causes the web-based interface to never be automatically refreshed.

Airlink Security

Specify the type of air link security to apply to this BHM:

- **Encryption Disabled** provides no encryption on the air link. This is the default mode.
- **Encryption Enabled** provides encryption, using a factory-programmed secret key that is unique for each module.

NOTE:
In any BH link where encryption is enabled, the BHS briefly drops registration and re-registers in the BHM every 24 hours to change the encryption key.

Authentication Mode

This parameter has no effect in the BHM. No BHS is ever required to authenticate in the BHM.

Authentication Key

Only if Authentication Required is selected in the Authentication Mode parameter, enter the hexadecimal key that will be exchanged between this BHM and the BHS.

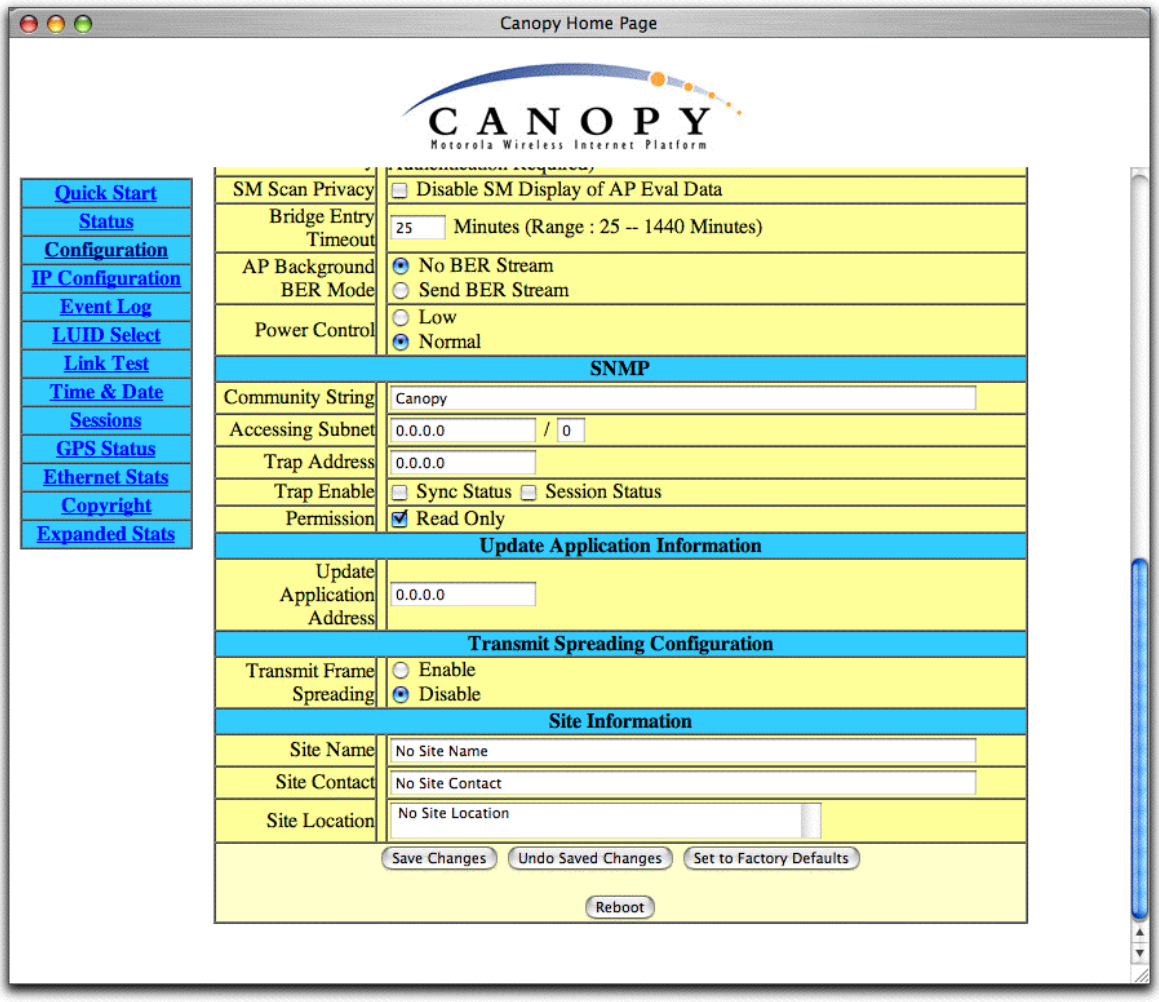


Figure 91: Configuration screen, BHM (continued)

As shown in Figure 91, the Configuration page continues with the following parameters.

SM Scan Privacy

When the SM Scan Privacy feature is enabled, you can use this field to suppress the display of data about this BHM on the AP Eval Data page of the registered BHS.

Bridge Entry Timeout

Specify the appropriate bridge timeout for correct network operation with the existing network infrastructure. The Bridge Entry Timeout should be a longer period than the ARP (Address Resolution Protocol) cache timeout of the router that feeds the network.

CAUTION!
An inappropriately low Bridge Entry Timeout setting may lead to temporary loss of communication with some end users.

AP Background BER Mode

Specify whether continuous BER (Bit Error Rate) data collection should be done. When **Send BER Stream** is selected for this parameter, you can read the bit error rate on the BHS side to assess the quality of a registered link. However, when **Send BER Stream** is selected, the aggregate available bandwidth decreases by approximately 200 kbps. For this reason, you should limit BER data collection to diagnostic intervals.

Power Control

In Release 4.1 and later releases, select either

- **Low** to set the BHM to operate at 18 dB less than full power to reduce the possibility of self-interference with a nearby module.
- **Normal** to allow the BHM to operate at full power.

CAUTION!
Selection of **Low** can cause a link to a distant BHS to drop. If a link drops when Power Control is set to low, the link can be re-established by only Ethernet access.

If you select **Low** and save the changes and reboot the BHM, you should immediately open the Link Test page and perform a link test.

Community String

Specify a control string that allows an Network Management Station (NMS) to access SNMP information. No spaces are allowed in this string. The default string is **Canopy**.

The **Community String** value is clear text and is readable by a packet monitor. Additional security derives from the configuration of the **Accessing Subnet**, **Trap Address**, and **Permission** parameters.

Accessing Subnet

Specify the addresses that are allowed to send SNMP requests to this BHM. The NMS has an address that is among these addresses (this subnet). You must enter both

- The network IP address in the form xxx.xxx.xxx.xxx
- The CIDR (Classless Interdomain Routing) prefix length in the form /xx

For example

- the /16 in 198.32.0.0/16 specifies a subnet mask of 255.255.0.0 (the first 16 bits in the address range are identical among all members of the subnet).
- 192.168.102.0 specifies that any device whose IP address is in the range 192.168.102.0 to 192.168.102.254 can send SNMP requests to the BHM, presuming that the device supplies the correct **Community String** value.

NOTE:
For more information on CIDR, execute an Internet search on “Classless Interdomain Routing.”

The default treatment is to allow all networks access.

Trap Address

Specify the IP address (xxx.xxx.xxx.xxx) of a Network Management Station (NMS) to which trap information should be sent. Trap information informs the NMS that something has occurred. For example, trap information is sent

- after a reboot of the module.
- when an NMS attempts to access agent information but either
  - supplied an inappropriate community string or SNMP version number.
  - is associated with a subnet to which access is disallowed.

Trap Enable

Select either **Sync Status** or **Session Status** to enable SNMP traps. If you select neither, then traps are disabled.

Permission

Select **Read Only** if you wish to disallow any parameter changes by the NMS.

Update Application Address

For capabilities in future software releases, you can enter the address of the server to access for software updates on this BHM.

Transmit Frame Spreading

If you select **Enable**, then a BHS between two BHMs can register in the assigned BHM (not the other BHM). Where the BHS operates on Release 4.0 or later, we strongly recommend that you select this option.

With this selection, the BHM does not transmit a beacon in each frame, but rather transmits a beacon in only pseudo-random frames in which the BHS expects the beacon. This allows multiple BHMs to send beacons to multiple BHSs in the same range without interference.

Site Name

Specify a string to associate with the physical module. This parameter is written into the *sysName* SNMP MIB-II object and can be polled by an NMS. The buffer size for this field is 128 characters.

Site Contact

Enter contact information for the module administrator. This parameter is written into the *sysContact* SNMP MIB-II object and can be polled by an NMS. The buffer size for this field is 128 characters.

Site Location

Enter information about the physical location of the module. This parameter is written into the *sysLocation* SNMP MIB-II object and can be polled by an NMS. The buffer size for this field is 128 characters.

The Configuration page also provides the following buttons.

Save Changes

When you click this button, any changes that you made on the Configuration page are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Undo Saved Changes

When you click this button, any changes that you made but were not committed by a reboot of the module are undone.

Set to Factory Defaults

When you click this button, *all configurable parameters on all configurable pages* are reset to the factory settings.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

Whenever you change a parameter in the Configuration page, the system highlights the **Reboot** button as a reminder that a reboot (in addition to a save) is required to implement the changes.

18.4.2 IP Configuration Page of the BHM

An example of a BHM IP Configuration screen is displayed in Figure 92.

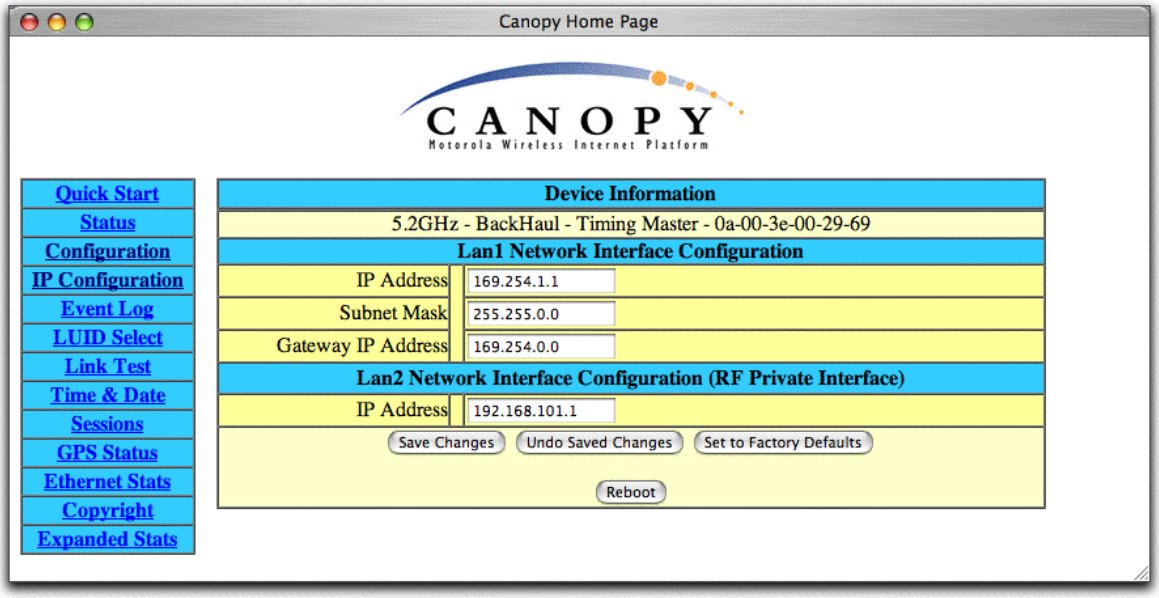


Figure 92: IP Configuration screen, BHM

You may set the following IP Configuration page parameters.

LAN1 Network Interface Configuration, IP Address

Enter the *non-routable* IP address to be associated with the Ethernet connection on this module. (The default IP address from the factory is 169.254.1.1.) If you set and then forget this parameter, then you must both

1. physically access the module.
2. use an override plug to electronically access the module configuration parameters at 169.254.1.1. See Overriding Forgotten IP Addresses or Passwords on AP, SM, or BH on Page 302.

RECOMMENDATION:
Note or print the IP settings from this page. Ensure that you can readily associate these IP settings both with the module and with the other data that you store about the module.

LAN1 Network Interface Configuration, Subnet Mask

Enter an appropriate subnet mask for the BHM to communicate on the network. The default subnet mask is 255.255.255.0. See Allocating Subnets on Page 123.

LAN1 Network Interface Configuration, Gateway IP Address

Enter the appropriate gateway for the BHM to communicate with the network. The default gateway is 169.254.0.0.

LAN2 Network Interface Configuration (RF Private Interface), IP Address

Enter the IP address to be associated with this BHM for over-the-air access.

The IP Configuration page also provides the following buttons.

Save Changes

When you click this button, any changes that you made on the IP Configuration page are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Undo Saved Changes

When you click this button, any changes that you made but were not committed by a reboot of the module are undone.

Set to Factory Defaults

When you click this button, *all configurable parameters on all configurable pages* are reset to the factory settings.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

Whenever you change a parameter in the IP Configuration page, the system highlights the **Reboot** button as a reminder that a reboot (in addition to a save) is required to implement the changes.

18.5 CONFIGURING A BH TIMING SLAVE FOR THE DESTINATION

18.5.1 Configuration Page of the BHS

An example of a BHS Configuration screen is displayed in Figure 93.

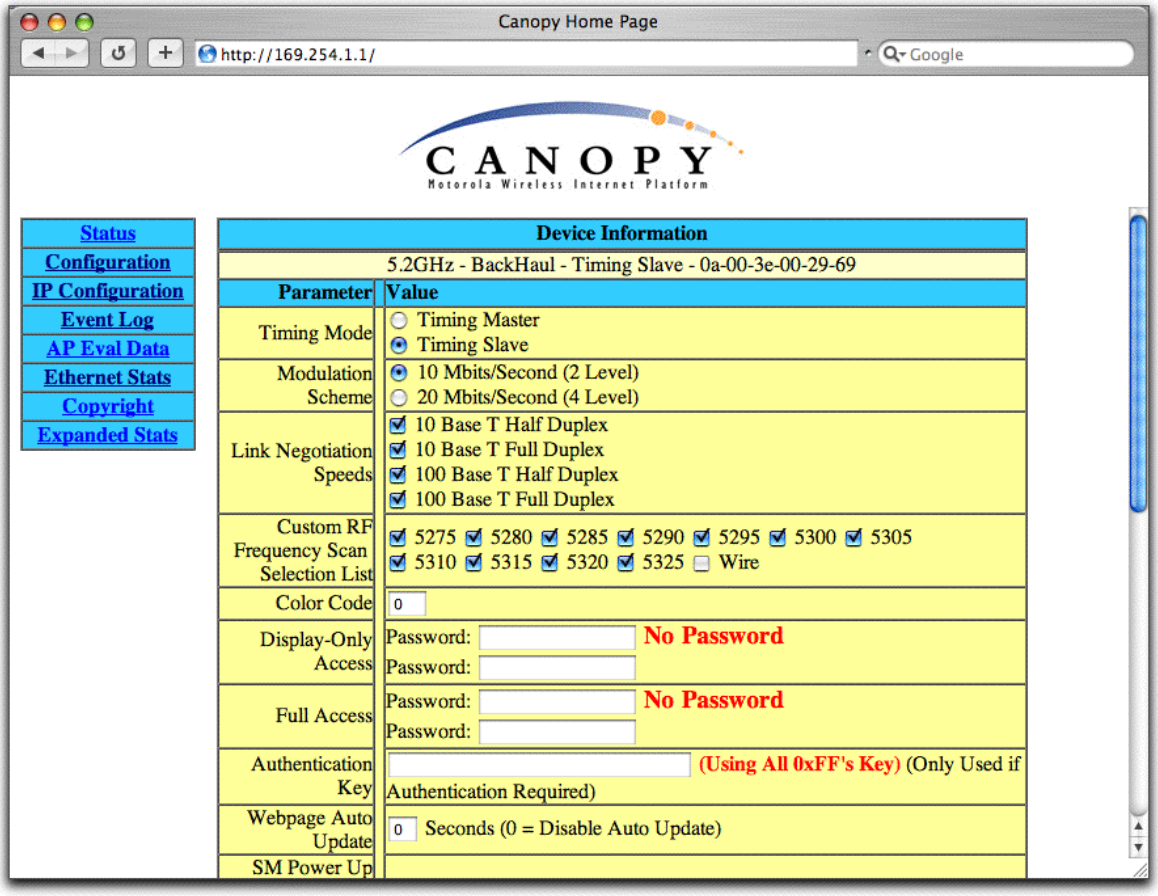


Figure 93: Configuration screen, BHS

The Configuration web page contains all of the configurable parameters that define how the module operates. The first line of information on the Configuration screen echoes the **Device Type** from the Status web page.

You may set the following Configuration page parameters.

Timing Mode

Select **Timing Slave**. This BH will receive sync from another source. Whenever you toggle this parameter to Timing Slave from Timing Master, you should also do the following:

1. Make no other changes in this or any other interface page.
2. Save this change of timing mode.
3. Reboot the BH.

RESULT: The set of interface web pages that is unique to a BHS is made available.

Modulation Scheme

This parameter is available for only the 20-Mbps BH. You can specify in this parameter whether to use this 20-Mbps BH as a 10-Mbps BH.

Link Negotiation Speeds

Specify the type of link speed for the Ethernet connection. The default for this parameter is that all speeds are selected. The recommended setting is a single speed selection for all APs, BHs, and SMs in the operator network.

Custom RF Frequency Scan Selection List

Specify the frequency that the BHS should scan to find the BHM. The frequency *band* of the BHs affects what channels you select.

IMPORTANT!

In the 2.4-GHz frequency band, the BHS can register to a BHM that transmits on a frequency 2.5 MHz higher than the frequency that the SM receiver locks when the scan terminates as successful. This establishes a poor-quality link. To prevent this, select frequencies that are at least 5 MHz apart.

In a 2.4-GHz BHS, this parameter displays all available channels, but has only three recommended channels selected by default. See 2.4-GHz AP Cluster Recommended Channels on Page 101.

In a 5.2- or 5.4-GHz BHS, this parameter displays only ISM frequencies. In a 5.7-GHz BHS, this parameter displays both ISM and U-NII frequencies. If you select all frequencies that are listed (default selections), then the module scans for a signal on any channel. If you select only one, then the module limits the scan to that channel. Since the frequencies that this parameter offers for each of these two bands are 5 MHz apart, a scan of *all* channels does not risk establishment of a poor-quality link as in the 2.4-GHz band. Nevertheless, this can risk establishment of a link to the wrong BHM.

A list of channels in the band is provided in Considering Frequency Band Alternatives on Page 100.

(The selection labeled **Factory** requires a special software key file for implementation.)

Color Code

The operator specifies a value from 0 to 254. For registration to occur, the color codes of the BHS and of the BHM *must* match. Color code is not a security feature. Instead, color code allows you to segregate an individual network or neighboring Canopy networks.

Color code also allows you to force a BHS to register to only a specific BHM, even if the BHS can reach multiple BHMs. On all Canopy modules, the default setting for the color code value is 0. This value matches only the color code of 0 (*not* all 255 color codes).

RECOMMENDATION:
Note the color code that you enter. Ensure that you can readily associate this color code both with the module and with the other data that you store about the module.

Display-Only Access

If you set (populate) the **Display-Only Access** password, this password will allow only *viewing* activities on the module.

This protection interacts with the **Full Access** password protection as follows:

- If the **Display-Only Access** password is set and the **Full Access** password *is not*, then the **Display-Only Access** password allows
  - telnet and FTP access to the module.
  - *viewing or changing* the parameters of the module. This configuration *is not* recommended.
- If the **Full Access** password is also set, then the **Full Access** password allows telnet and FTP access to the module, and the **Display-Only Access** password does not.
- If the **Display-Only Access** password *is not* set and the **Full Access** password is, then no password is required to view the parameters of the module.
- If neither password is set, then anyone can *view or change* the parameters of the module. This configuration *is not* recommended.

To set this password, enter the same expression in both **Display-Only Access** fields for verification. When the web-based interface prompts for this password, no user name is required. However, when a telnet or FTP session prompts for this password, you must enter the user name `root` in addition to the password.

If you set and then forget the **Display-Only Access** password, then you must both

1. physically access the module.
2. use an override plug to electronically access the module configuration parameters at 169.254.1.1. See Overriding Forgotten IP Addresses or Passwords on AP, SM, or BH on Page 302.

Full Access

If you set the **Full Access** password, this password will allow

- telnet and FTP access to the module.
- *viewing or changing* the parameters of the module.

To set this password, enter the same expression in both **Full Access** fields for verification. When the web-based interface prompts for this password, no user name is required. However, when a telnet or FTP session prompts for this password, you must enter the user name `root` in addition to the password.

If you set and then forget the **Full Access** password, then you must both

1. physically access the module.
2. use an override plug to electronically access the module configuration parameters at 169.254.1.1. See Overriding Forgotten IP Addresses or Passwords on AP, SM, or BH on Page 302.

NOTE:
You can unset either password (revert the access to no password required). To do so, type a space into the field and reboot the module. You must enter any password twice to allow the system to verify that the password is not mistyped. After any password is set and a reboot of the module has occurred, a **Password Set** indicator appears to the right of the field.

RECOMMENDATION:
Note the passwords that you enter. Ensure that you can readily associate these passwords both with the module and with the other data that you store about the module.

Authentication Key

Enter the hexadecimal key that will be exchanged between this BHS and the BHM. This field is used only if the BHM is configured to require authentication.

Webpage Auto Update

Enter the frequency (in seconds) for the web browser to automatically refresh the web-based interface. The default setting is 0. The 0 setting causes the web-based interface to never be automatically refreshed.

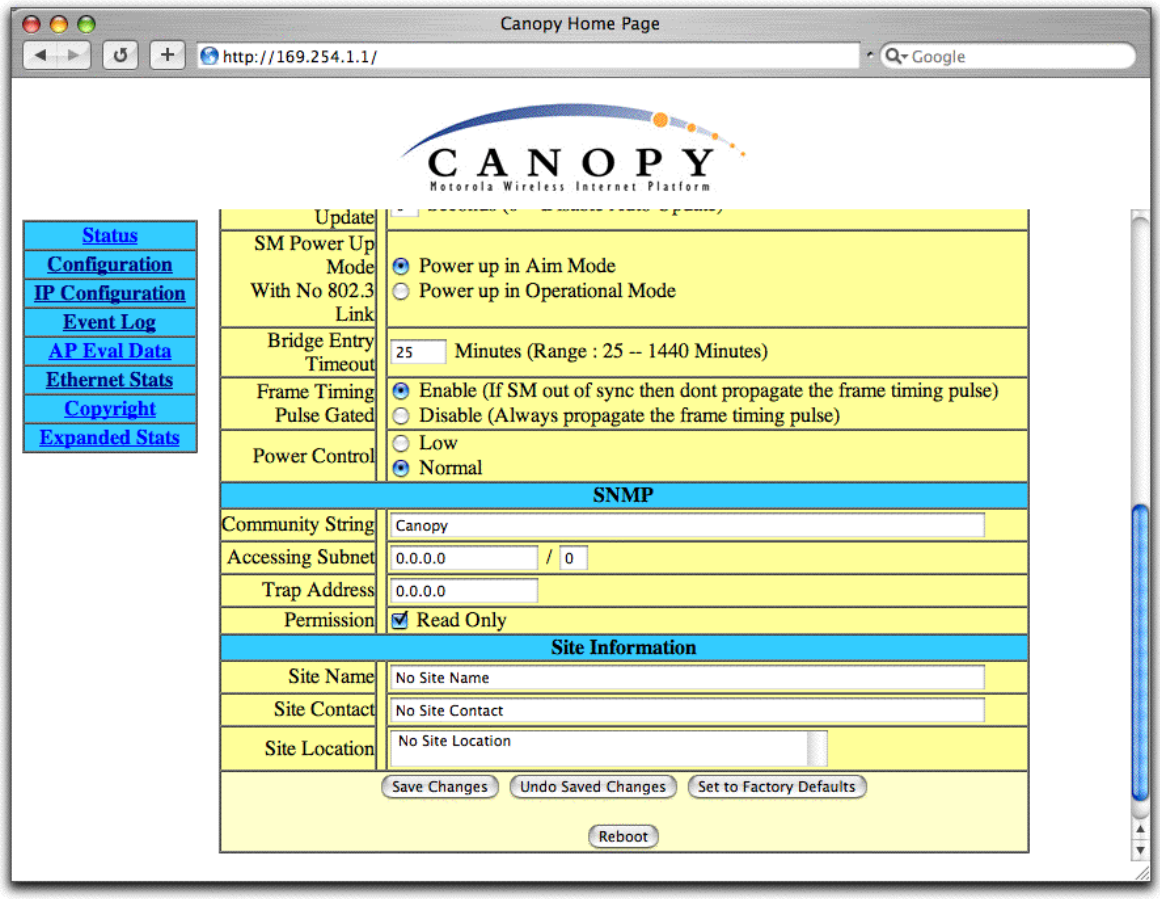


Figure 94: Configuration screen, BHS (continued)

As shown in Figure 94, the Configuration page continues with the following parameters.

SM Power Up Mode With No 802.3 Link

Specify the default mode in which this BHS will power up when the BHS senses no Ethernet link. Select either

- **Power Up in Aim Mode**—the BHS boots in an aiming mode. When the BHS senses an Ethernet link, this parameter is automatically reset to Power Up in Operational Mode. When the BHS senses no Ethernet link within 15 minutes after power up, the BHS carrier shuts off.
- **Power Up in Operational Mode**—the BHS boots in Operational mode and attempts registration. This is the default selection.

Bridge Entry Timeout

Specify the appropriate bridge timeout for correct network operation with the existing network infrastructure. Timeout occurs when the BHM encounters no activity with the BHS (whose MAC address is the bridge entry) within the interval that this parameter specifies. The Bridge Entry Timeout should be a longer period than the ARP (Address Resolution Protocol) cache timeout of the router that feeds the network.

This parameter governs the timeout interval, even if a router in the system has a longer timeout interval. The default value of this field is 25 minutes.

CAUTION!
An inappropriately low Bridge Entry Timeout setting may lead to temporary loss of communication with some end users.

Frame Timing Pulse Gated

If this BHS extends the sync pulse to a BHM or an AP, select either

- **Enable**—If this BHS loses sync, then *do not* propagate a sync pulse to the BHM or AP. This setting prevents interference in the event that the SM loses sync.
- **Disable**—If this BHS loses sync, then propagate the sync pulse to the BHM or AP.

See Wiring to Extend Network Sync on Page 294.

Power Control

In Release 4.1 and later releases, select either

- **Low** to set the BHS to operate at 18 dB less than full power to reduce the possibility of self-interference with a nearby module.
- **Normal** to allow the BHS to operate at full power.

CAUTION!
Selection of **Low** can cause a link to a distant BHM to drop. If a link drops when Power Control is set to low, the link can be re-established by only Ethernet access.

If you select **Low** and save the changes and reboot the AP, you should immediately open the Link Test page and perform a link test.

Community String

Specify a control string that allows a NMS (Network Management Station) to access MIB information about this BHS. No spaces are allowed in this string. The default string is **Canopy**.

The **Community String** value is clear text and is readable by a packet monitor. Additional security derives from the configuration of the **Accessing Subnet**, **Trap Address**, and **Permission** parameters.

Accessing Subnet

Specify the addresses that are allowed to send SNMP requests to this BHS. The NMS has an address that is among these addresses (this subnet). You must enter both

- The network IP address in the form xxx.xxx.xxx.xxx
- The CIDR (Classless Interdomain Routing) prefix length in the form /xx

For example

- the /16 in 198.32.0.0/16 specifies a subnet mask of 255.255.0.0 (the first 16 bits in the address range are identical among all members of the subnet).
- 192.168.102.0 specifies that any device whose IP address is in the range 192.168.102.0 to 192.168.102.254 can send SNMP requests to the BHS, presuming that the device supplies the correct **Community String** value.

NOTE:
For more information on CIDR, execute an Internet search on “Classless Interdomain Routing.”

The default treatment is to allow all networks access (set to 0).

Trap Address

Specify the IP address (xxx.xxx.xxx.xxx) of an NMS to which trap information should be sent. Trap information informs the NMS that something has occurred. For example, trap information is sent:

- after a reboot of the module.
- when an NMS attempts to access agent information but either
  - supplied an inappropriate community string or SNMP version number.
  - is associated with a subnet to which access is disallowed.

Permission

Select **Read Only** if you wish to disallow any parameter changes by the NMS.

Site Name

Specify a string to associate with the physical module. This parameter is written into the *sysName* SNMP MIB-II object and can be polled by an NMS. The buffer size for this field is 128 characters.

Site Contact

Enter contact information for the module administrator. This parameter is written into the *sysContact* SNMP MIB-II object and can be polled by an NMS. The buffer size for this field is 128 characters.

Site Location

Enter information about the physical location of the module. This parameter is written into the *sysLocation* SNMP MIB-II object and can be polled by an NMS. The buffer size for this field is 128 characters.

The Configuration page also provides the following buttons.

Save Changes

When you click this button, any changes that you made on the Configuration page are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Undo Saved Changes

When you click this button, any changes that you made but were not committed by a reboot of the module are undone.

Set to Factory Defaults

When you click this button, *all configurable parameters on all configurable pages* are reset to the factory settings.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

Whenever you change a parameter in the Configuration page, the system highlights the **Reboot** button as a reminder that a reboot (in addition to a save) is required to implement the changes.

18.5.2 IP Configuration Page of the BHS

An example of the BHS IP Configuration page is displayed in Figure 95.

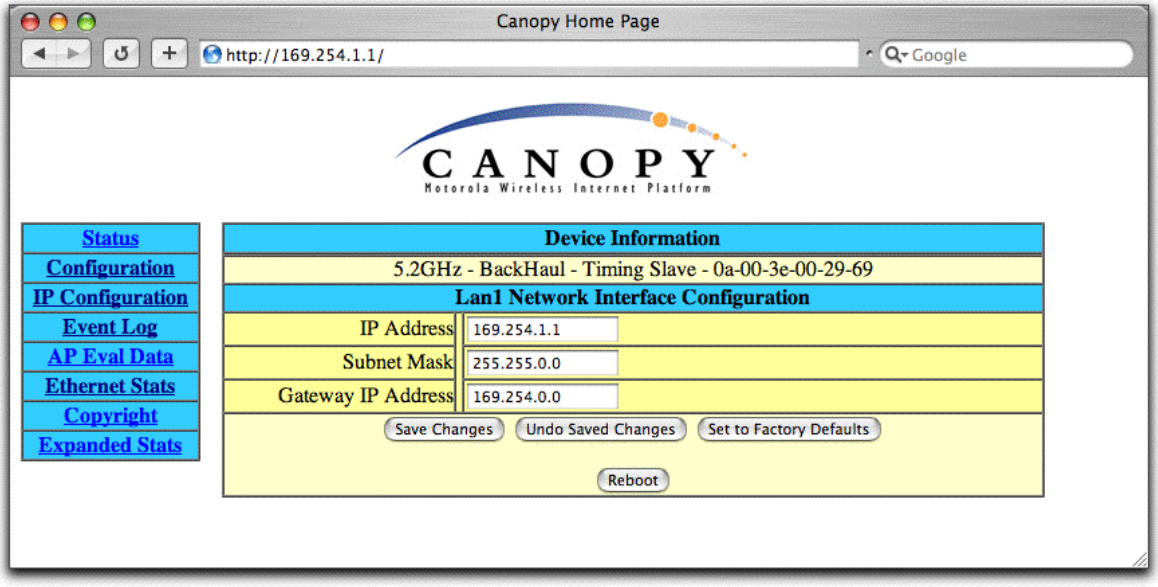


Figure 95: IP Configuration screen, BHS

You may set the following IP Configuration page parameters.

LAN1 Network Interface Configuration, IP Address

Enter the *non-routable* IP address to associate with the Ethernet connection on this BHS. (The default IP address from the factory is 169.254.1.1.) If you set and then forget this parameter, then you must both

1. physically access the module.
2. use an override plug to electronically access the module configuration parameters at 169.254.1.1. See Overriding Forgotten IP Addresses or Passwords on AP, SM, or BH on Page 302.

RECOMMENDATION:
Note or print the IP settings from this page. Ensure that you can readily associate these IP settings both with the module and with the other data that you store about the module.

LAN1 Network Interface Configuration, Subnet Mask

Enter an appropriate subnet mask for the BHS to communicate on the network. The default subnet mask is 255.255.255.0. See Allocating Subnets on Page 123.

LAN1 Network Interface Configuration, Gateway IP Address

Enter the appropriate gateway for the BHS to communicate with the network. The default gateway is 169.254.0.0.

The IP Configuration page also provides the following buttons.

Save Changes

When you click this button, any changes that you made on the IP Configuration page are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Undo Saved Changes

When you click this button, any changes that you made but were not committed by a reboot of the module are undone.

Set to Factory Defaults

When you click this button, *all configurable parameters on all configurable pages* are reset to the factory settings.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

Whenever you change a parameter in the IP Configuration page, the system highlights the **Reboot** button as a reminder that a reboot (in addition to a save) is required to implement the changes.

18.6 ADJUSTING TRANSMITTER OUTPUT POWER

Authorities may require transmitter output power levels to be adjustable and/or lower than the highest that a module produces. Canopy 2.4-GHz modules with Release 4.2.7 or later and 5.4-GHz modules include a Configuration page parameter to reduce power on an infinite scale to achieve compliance.

The professional installer of Canopy equipment has the responsibility to

- maintain awareness of applicable regulations.
- calculate the permissible transmitter output power for the module.
- confirm that the initial power setting is compliant.
- confirm that the power setting is compliant following any reset of the module to factory defaults.

The calculation of transmitter output power is as follows:

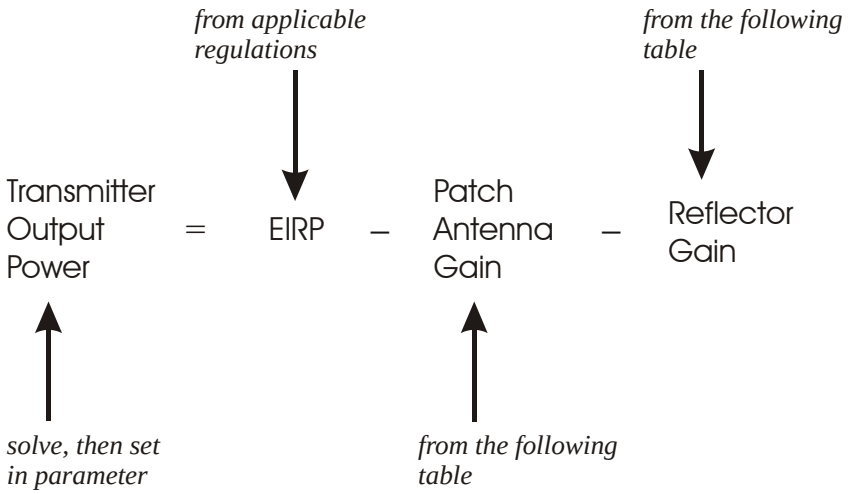


Table 44: Patch antenna and reflector gain

Frequency Band Range	Gain	
	Patch Antenna	Reflector
2.4 GHz	8 dBi	11dBi
5.2, 5.4, or 5.7 GHz	7 dBi	18dBi

19 INSTALLING COMPONENTS

RECOMMENDATION:
Use *shielded* cable for all Canopy infrastructure connections associated with BHs, APs, and CMMs. The environment that these modules operate in often has significant unknown or varying RF energy. Operator experience consistently indicates that the additional cost of shielded cables is more than compensated by predictable operation and reduced costs for troubleshooting and support.

19.1 PDA ACCESS TO CANOPY MODULES

For RF spectrum analysis or module aiming on a roof or tower, a personal digital assistant (PDA) is easier to carry than, and as convenient to use as, a notebook computer. In Release 4.2 and later releases, the PDA is more convenient to use than in previous releases because no scrolling is required to view

- spectrum analysis results.
- received signal strength indicator (RSSI) and jitter. (See Figure 96.)
- AP evaluation data. (See Figure 97.)
- information that identifies the module, software, and firmware. (See Figure 98.)

To access this data in a format the fits a 320 x 240 pixel PDA screen, the PDA must have all of the following:

- a Compact Flash card slot.
- any of several Compact Flash wired Ethernet cards.
- a wired Ethernet connection to the module.
- a browser directed to http://*ModuleIPAddress*/pda.html.

The initial page shows signal information as in Figure 96. For additional information about the Spectrum Analyzer feature in an SM or BHS, see Monitoring the RF Environment on Page 285.

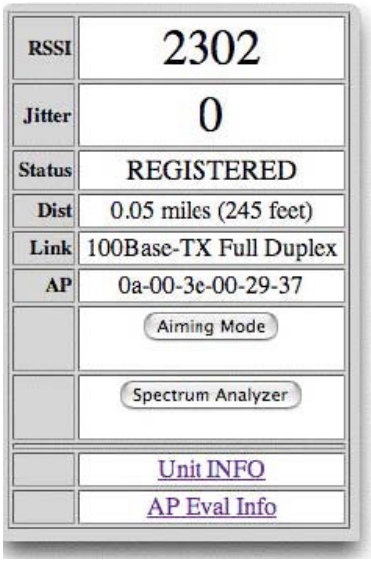


Figure 96: Signal information screen for PDA access, Release 4.2

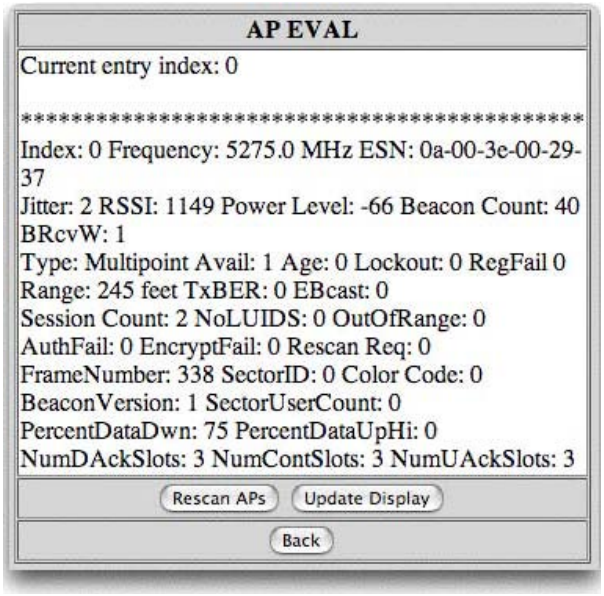

AP EVAL
Current entry index: 0
****
Index: 0 Frequency: 5275.0 MHz ESN: 0a-00-3e-00-29-37
Jitter: 2 RSSI: 1149 Power Level: -66 Beacon Count: 40
BRcvW: 1
Type: Multipoint Avail: 1 Age: 0 Lockout: 0 RegFail 0
Range: 245 feet TxBER: 0 EBcast: 0
Session Count: 2 NoLUIDS: 0 OutOfRange: 0
AuthFail: 0 EncryptFail: 0 Rescan Req: 0
FrameNumber: 338 SectorID: 0 Color Code: 0
BeaconVersion: 1 SectorUserCount: 0
PercentDataDwn: 75 PercentDataUpHi: 0
NumDAckSlots: 3 NumContSlots: 3 NumUAckSlots: 3
Rescan APs
Update Display
Back

Figure 97: AP Evaluation screen for PDA access, Release 4.2

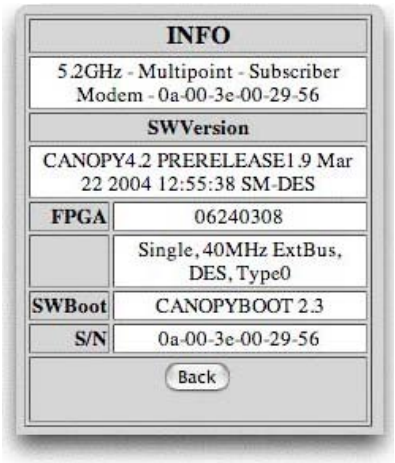


Figure 98: Module information screen for PDA access, Release 4.2

19.2 INSTALLING AN AP

To install the Canopy AP, perform the following steps.

Procedure 23: Installing the AP

1. Begin with the AP in the powered-down state.
2. Choose the best mounting location for your particular application. Modules need not be mounted next to each other. They can be distributed throughout a given site. Mounting can be done with stainless steel hose clamps or another equivalent fastener.
   NOTE: Canopy products offer no software utility for alignment of APs or Backhaul timing master modules.
3. Align the AP as follows:
   a. Move the module to where the link will be unobstructed by the radio horizon and no objects penetrate the Fresnel zone. (The Canopy System Calculator page AntennaElevationCalcPage.xls automatically calculates the minimum antenna elevation that is required to extend the radio horizon to the other end of the link. The Canopy System Calculator page FresnelZoneCalcPage.xls automatically calculates the Fresnel zone clearance that is required between the visual line of sight and the top of a high-elevation object.)
   b. Use a local map, compass, and/or GPS device as needed to determine the direction that one or more APs require to each cover the intended 60° sector.
   c. Apply the appropriate degree of downward tilt. (The Canopy System Calculator page DowntiltCalcPage.xls automatically calculates the angle of antenna downward tilt that is required.)
   d. Ensure that the nearest and furthest SMs that must register to this AP are within the beam coverage area. (The Canopy System Calculator page BeamwidthRadiiCalcPage.xls automatically calculates the radii of the beam coverage area.)
4. Using stainless steel hose clamps or equivalent fasteners, lock the AP in the proper direction and downward tilt.

5. Remove the base cover of the AP. (See Figure 47 on Page 132.)
6. Attach the cables to the AP.
(See Procedure 5 on Page 138.)

NOTE: When power is applied to a Canopy module or the unit is reset on the web-based interface, the module requires approximately 25 seconds to boot. During this interval, self-tests and other diagnostics are being performed. See Table 35 on Page 133.

========== **end of procedure** ==========

19.3 INSTALLING A CONNECTORIZED FLAT PANEL ANTENNA

To install a connectorized flat panel antenna to a mast or structure, follow instructions that the manufacturer provides. Install the antenna safely and securely, consistent with industry practices.

The Universal Mounting Bracket available from Motorola (Part Number SMMB-1 and consisting of a mounting bracket and L-shaped aluminum tube) holds one Canopy module, but cannot hold both the module and a connectorized antenna.

IMPORTANT!
Connectorized antennas *require* professional installation.

The professional installer is responsible for

- selection of an antenna that the regulatory agency has approved for use with the Canopy 900-MHz AP and SM.
- setting of the gain consistent with regulatory limitations and antenna specifications.
- use of moisture sealing tape or wrap to provide long-term integrity for the connection.

AP Configuration parameters for the connected antenna are described under

- Max Range on Page 195.
- External Filters Delay on Page 196.

19.4 INSTALLING A GPS ANTENNA

The following information describes the recommended tools and procedures to mount the GPS antenna.

Recommended Tools for GPS Antenna Mounting

The following tools may be needed for mounting the GPS antenna:

- 3/8” nut driver

- 12” adjustable wrench
- 7/16” wrench
- Needle-nose pliers

Mounting a GPS Antenna

Perform the following procedure to mount a GPS antenna.

Procedure 24: Mounting the GPS antenna

1. Ensure that the mounting position
   - has an unobstructed view of the sky to 20º above the horizon.
   - *is not* the highest object at the site. (This is important for lightning protection.)
   - *is not* further than 100 feet (30.4 meters) of cable from the CMM2.
2. Select a pole that has an outside diameter of 1.25 to 1.5 inches (3 to 4 cm) to which the flange of the GPS antenna can be mounted.
3. Place the U-bolts (provided) around the pole as shown in Figure 99.
4. Slide the GPS antenna flange onto the U-bolts.
5. Slide the ring washers (provided) onto the U-bolts.
6. Slide the lock washers (provided) onto the U-bolts.
7. Use the nuts (provided) to securely fasten the flange to the U-bolts.

end of procedure

Figure 99: Detail of GPS antenna mounting

19.4.1 Recommended Materials for Cabling the GPS Antenna

The following materials are required for cabling the GPS antenna:

- 100 feet (30.4 meters) of LMR200 coaxial cable

- 2 Times Microwave N-male connectors (Times Microwave P/N TC-200-NM) or equivalent connectors.

19.4.2 Cabling the GPS Antenna

Connect the GPS coax cable to the female N-connector on the GPS antenna.

19.5 INSTALLING A CMM2

Ensure that you comply with standard local or national electrical and climbing procedures when you install the CMM2.

19.5.1 CMM2 Installation Temperature Range

Install the CMM2 outside only when temperatures are above –4° F (–20° C). The bulkhead connector and the bushings and inserts in the bulkhead connector are rated for the full –40° to +131° F (–40° to +55° C) range of the CMM2. However, for dynamic operations (loosening, tightening, and inserting), they are compliant at, and rated for, only temperatures at or above –4° F (–20° C).

19.5.2 Recommended Tools for Mounting a CMM2

The following tools may be needed for mounting the CMM2:

- 3/8” nut driver
- 12” adjustable wrench
- 14-mm wrench for pole-mounting
- needle-nose pliers

19.5.3 Mounting a CMM2

Perform the following procedure to mount the CMM2.

Procedure 25: Mounting the CMM2

1. Ensure that the mounting position
   - *is not* further than 328 feet (100 meters) from the furthest AP or BH that the CMM2 will serve.
   - *is not* closer than 10 feet (3 meters) to the nearest AP or BH.
   - *is not* further than 100 feet (30.4 meters) of cable from the intended mounting position of the GPS antenna.
   - allows you to fully open the door of the CMM2 for service.
2. Select a support structure to which the flanges of the CMM2 can be mounted.
3. If the support structure is a wall, use screws or bolts (neither is provided) to attach the flanges to the wall.
4. If the support structure is an irregular-shaped object, use adjustable stainless steel bands (provided) to attach the CMM2 to the object.

5. If the support structure is a pole that has an outside diameter of 3 to 8 cm, or 1.25 to 3 inches, use a toothed V-bracket (provided) to
   a. attach the V-bracket to the pole as shown in Figure 100.
   b. attach the CMM2 flanges to the V-bracket.

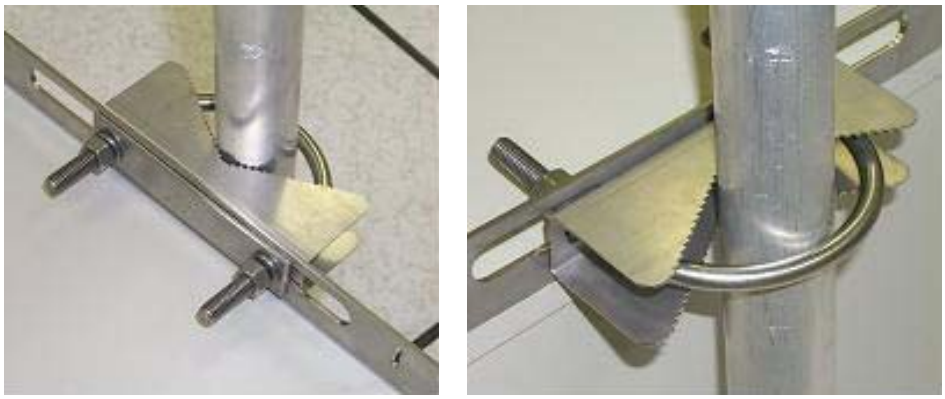


Figure 100: Detail of pole mounting

========== **end of procedure** ==========

19.5.4 Cabling a CMM2

> ***IMPORTANT!***
> Where you deploy CMM2s, one AP in each AP cluster must be connected to the master port on the CMM2, and each module connected to a CMM2 must be configured to **Sync to Received Signal (Timing Port)**. If either is not done, then the GPS receiver sends no sync pulse to the remaining ports.

Perform the following procedure to attach the CMM2 cables on both ends:

Procedure 26: Cabling the CMM2

1. Remove the base cover from any AP or BH that is to be connected to this CMM2. See Figure 47 on Page 132.
2. Remove the GPS sync cable knockout from the base cover.
3. For any AP that is to be connected to this CMM2, set the AP **Sync Input** Configuration Page parameter to the **Sync to Received Signal (Timing Port)** selection.
4. Review the schematic drawing inside the CMM2.

CAUTION!
Failure to perform the following step can result in damage to equipment.

5. Set the 115-/230-volt power switch in the CMM2 consistent with the power source. See Figure 101.

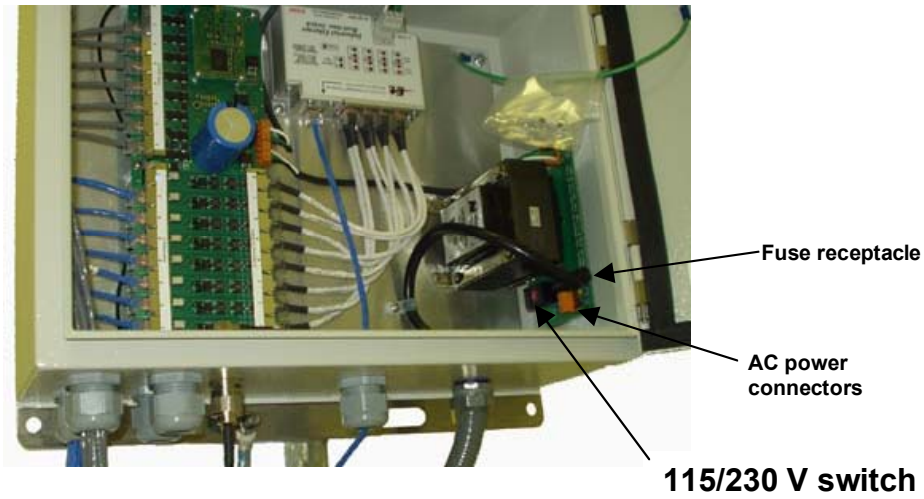


Figure 101: Location of 115-/230-volt switch

IMPORTANT!
The AC power connectors are labeled **N** for Neutral, **L** for Line, and **PE** for Protective Earth (PE) ⏚ or ground. The maximum thickness of wire to be used is 4 mm^2 or 12 AWG.

6. Route the Ethernet cables from the APs and or BHs to the CMM2.

   The strain relief plugs on the CMM2 have precut holes. Each hole of the strain relief is designed to hold two CAT 5 UTP cables or one shielded cable. The Ethernet cables have RJ-45 (standard Ethernet) connectors that mate to corresponding ports inside the CMM2.

   These ports are labeled **J3**. Eight J3 ports are available on the CMM2 to accommodate any combination of APs and BHs.

The logical connections in the CMM2 are displayed in Figure 102.

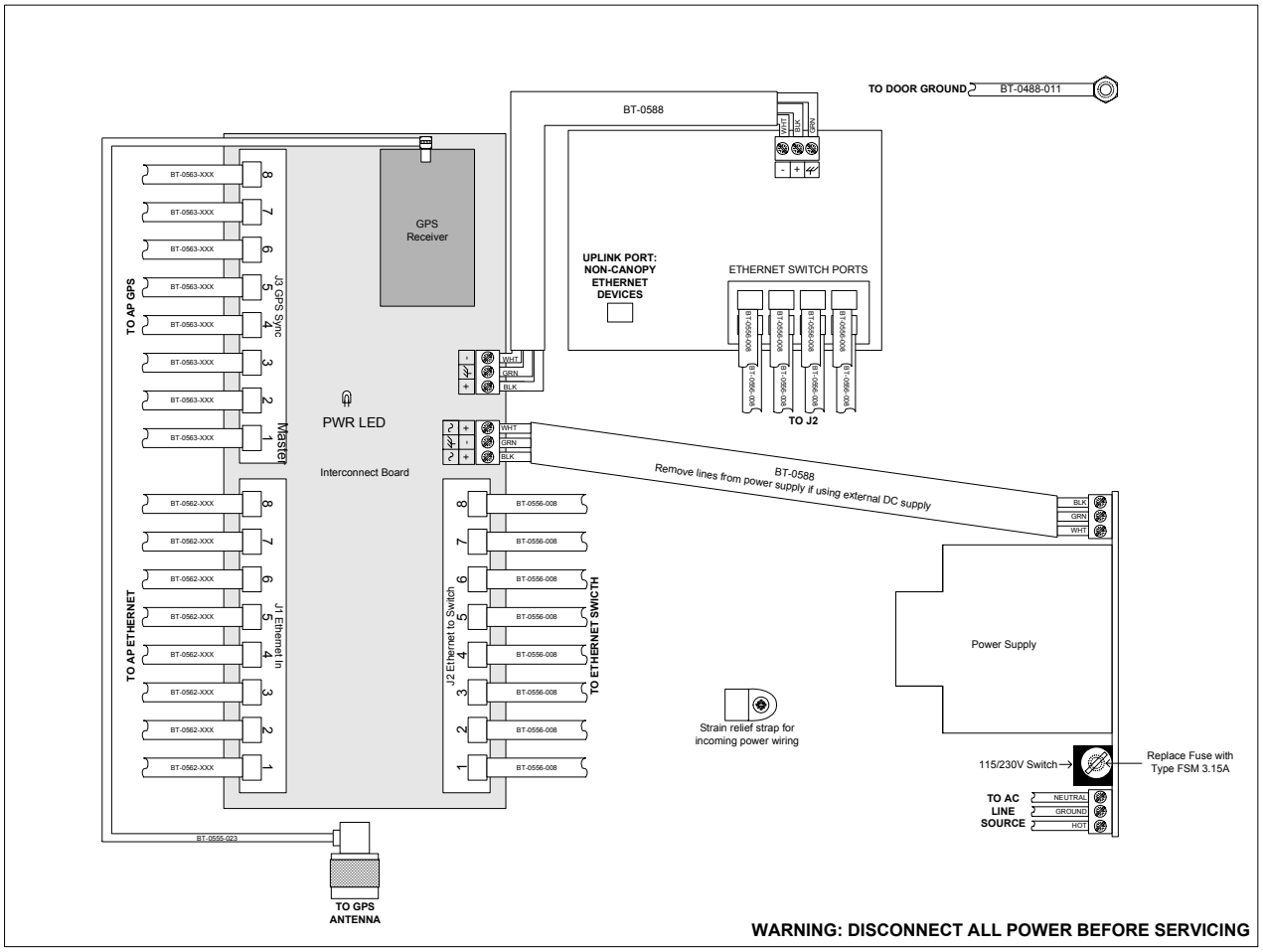


Figure 102: Layout of logical connections in CMM2

7. Connect the Ethernet cable from the first AP or BH to the **Port 1** in the J3 ports in the CMM2. This port is the *master* Ethernet port for the CMM2 and should be connected first in all cases. Figure 103 on Page 266 is a photograph of a properly wired CMM2.

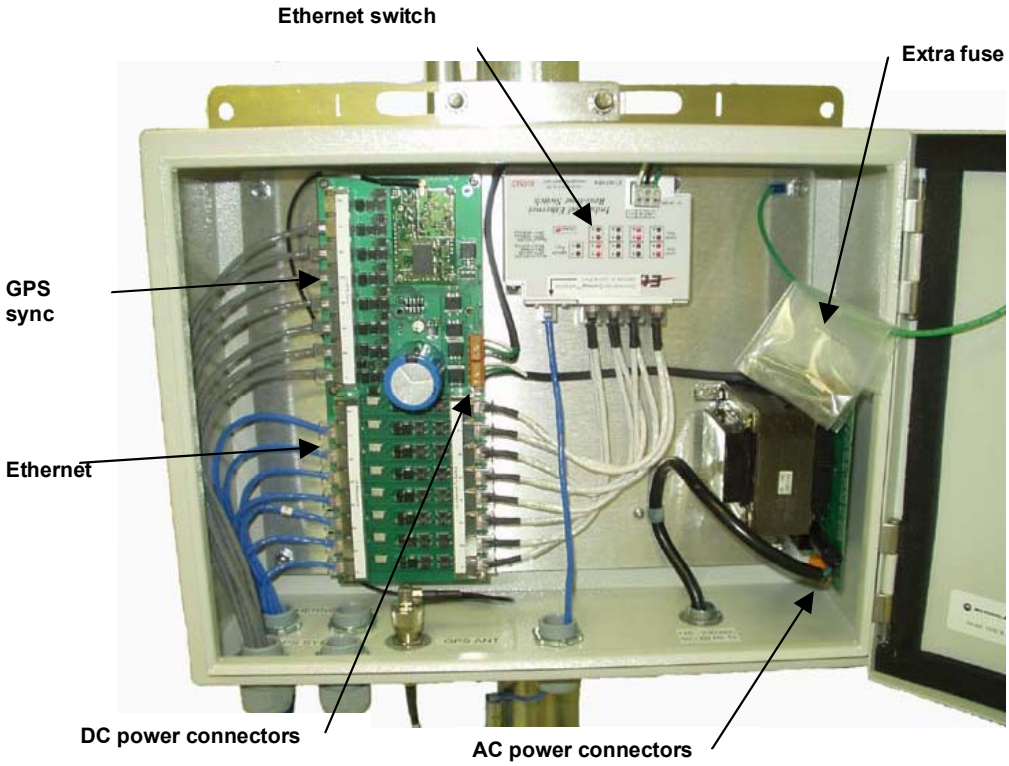


Figure 103: Canopy CMM2, front view

8. Connect the remaining Ethernet cables to the remaining J3 ports.
9. Route the GPS sync (serial) cables from the APs to the CMM2.

   The GPS sync cables have 6-conductor RJ-11 connectors that mate to corresponding ports inside the CMM2.

   These ports are labeled **J1**. Eight J1 ports are available on the CMM2 to accommodate any combination of APs and BHs.
10. Connect the GPS sync cable from the first AP or BH to the **Port 1** in the J1 ports in the CMM2. See Figure 103 on Page 266.

    This port is the *master* GPS sync port for the CMM2 and should be connected first in all cases. This is necessary to initialize the GPS on the CMM2.
11. Connect the remaining GPS sync cables to the remaining J1 ports.
12. If this CMM2 requires network connection, perform the following steps:
    c. Route a network cable into the CMM2.
    d. Connect to the uplink port on the switch.
    e. Properly ground (connect to Protective Earth [PE] ⏚) the Ethernet cable. The Canopy Surge Suppressor provides proper grounding for this situation.

NOTE: Instructions for installing a Canopy Surge Suppressor are provided in Procedure 32 on Page 271.

13. Connect GPS coaxial cable to the N-connector on the outside of the CMM2. See Figure 48 on Page 134.
14. Connect AC or DC power to the CMM2, consistent with Figure 102 on Page 265. When power is applied, the following indicators are lighted:
    - the power LED on the Ethernet switch
    - the green LED on the circuit board, as shown in Figure 104.

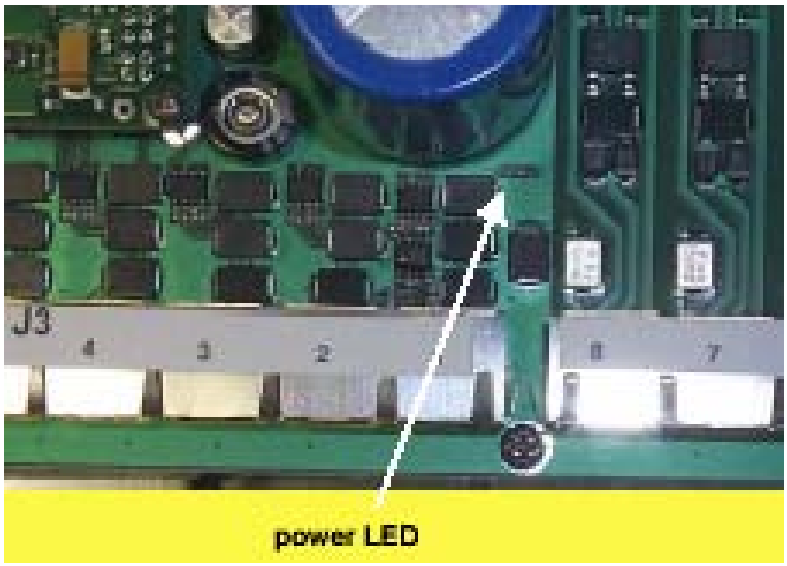


Figure 104: Port indicator LED on Ethernet switch

15. Verify that each port indicator LED on the Ethernet switch is lit (each AP or BH is reliably connected to the Ethernet switch).
16. Replace the base cover on each AP or BH.
17. Close and lock the CMM2.

========== **end of procedure** ==========

19.5.5 Verifying CMM2 Connections

To verify the CMM2 connections after the APs and or BHs have been installed, perform the following steps:

Procedure 27: Verifying CMM2 Connections

1. Access the web-based interface for each AP or BH by opening http://<ip-address>, where the <*ip-address*> is the address of the individual module.
2. In the Status page, verify that the time is expressed in GMT.
3. In the menu on the left-hand side of the web page, click on **GPS Status**.

4. Verify that the AP or BH is seeing and tracking satellites. (To generate the timing pulse, the module must track at least 4 satellites.)

end of procedure

19.6 INSTALLING A CMMmicro

Ensure that you comply with standard local or national electrical and climbing procedures when you install the CMMmicro.

19.6.1 CMMmicro Installation Temperature Range

Install the CMMmicro outside only when temperatures are above –4° F (–20° C). The bulkhead connector and the bushings and inserts in the bulkhead connector are rated for the full –40° to +131° F (–40° to +55° C) range of the CMMmicro. However, for dynamic operations (loosening, tightening, and inserting), they are compliant at, and rated for, only temperatures at or above –4° F (–20° C).

19.6.2 Recommended Tools for Mounting a CMMmicro

The following tools may be needed during installation:

- 3/8” nut driver
- 12” adjustable wrench
- 14-mm wrench for installation of pole-mounting brackets
- needle-nose pliers

19.6.3 Mounting a CMMmicro

Perform the following procedure to mount the CMMmicro.

Procedure 28: Mounting the CMMmicro

1. Ensure that the mounting position
   - *is not* further than 328 feet (100 meters) from the furthest AP or BH that the CMMmicro will serve.
   - *is not* closer than 10 feet (3 meters) to the nearest AP or BH.
   - *is not* further than 100 feet (30.5 meters) of cable from the intended mounting position of the GPS antenna.
   - allows you to fully open the door of the CMMmicro for service.
2. Select a support structure to which the flanges of the CMMmicro can be mounted.
3. If the support structure is a wall, use screws or bolts (neither is provided) to attach the flanges to the wall.

   If the support structure is an irregular-shaped object, use adjustable stainless steel bands (provided) to attach the CMMmicro to the object.

4. If the support structure is a pole that has an outside diameter of 1.25 to 3 inches (3 to 8 cm), use a toothed V-bracket (provided) to
   a. attach the V-bracket to the pole as shown in Figure 100 on Page 263.
   b. attach the CMMmicro flanges to the V-bracket.

end of procedure

19.6.4 Installing the Power Supply for the CMMmicro

Install the CMMmicro power converter in only a hut, wiring closet, or weatherized enclosure.

WARNING!

Although the output of the power converter is 24 V, the 100-W power rating classifies the converter as a Class 2 electric device. For this reason, whenever you work on power in the CMMmicro, you must *first* disconnect the CD converter from the AC power source.

Perform the following procedure to install the provided power supply.

Procedure 29: Installing the Power Supply for the CMMmicro

1. Connect the 6-ft (2-m) AC power cord to the power converter (but not yet to an AC receptacle).
2. Select the length of power cord as follows:
   a. If either mounting the CMMmicro inside with the power converter or outside within 9 ft (2.8 m) of the power converter, select the 10-ft (3-m) DC power cord (rated for outdoor use).
   b. If mounting the CMMmicro outside and further than 9 ft (2.8 m) from the power converter, ensure that this additional length of cord is either UV-resistant or shielded from UV rays.

DC Power Cord Length	Proper Wire Size
270 ft (~80 m)	12 AWG (4 mm^2)
450 ft (~140 m)	10 AWG (6 mm^2)
675 ft (~205 m)	8 AWG (10 mm^2)
950 ft (~290 m)	6 AWG (16 mm^2)

   - use a terminal block, connector, or splice to add the additional length.
   - protect the terminal block, connector, or splice (as inside a weatherized enclosure, for example).

3. Feed the power cord through the bulkhead connector of the CMMmicro.
4. Connect the converter lead whose insulation has a white stripe to +V on the CMMmicro terminal block.
5. Connect the converter lead whose insulation is solid black to -V on the CMMmicro terminal block.

========== **end of procedure** ==========

19.6.5 Cabling a CMMmicro

Perform the following procedure to attach the CMMmicro cables on both ends:

Procedure 30: Cabling the CMMmicro

1. Remove the base cover from any AP or BH that is to be connected to this CMMmicro. See Figure 47 on Page 132.
2. Review the schematic drawing inside the CMMmicro.
3. Note that the inserts in the bulkhead connector bushings have precut holes.
4. Route the Ethernet cables from the APs through the bulkhead connectors to the Ethernet switch in the CMMmicro.
5. If the BH at this site is a 45-Mbps BH
   a. connect the BH outdoor unit (ODU) to the ODU port of the power indoor unit (PIDU).
   b. connect the PIDU to an unpowered port of the CMMmicro.
6. If the BH is other than a 45-Mbps BH, route the Ethernet cables from the BH through the bulkhead connectors to the Ethernet switch in the CMMmicro.
7. If the site has a wired network feed, route the cable into the CMMmicro and connect it to an *unpowered* port on the switch.
8. Mount a Canopy surge suppressor at a low point of the network feed and connect the surge suppressor to solid ground.
9. On the door label, record the MAC and IP addresses of the CMMmicro and all connected equipment.
10. Consistent with practices in your company, note the above information to add later to the company equipment database.
11. Connect the GPS coax cable from the GPS antenna to the female BNC connector in the CMMmicro.
12. If this CMMmicro requires network connection, perform the following steps:
    a. Route a network cable into the CMMmicro.
    b. Connect to the uplink port on the switch.
    c. Properly ground (connect to Protective Earth [PE] ⏚) the Ethernet cable. The Canopy Surge Suppressor provides proper grounding for this situation.
    NOTE: Instructions for installing a Canopy Surge Suppressor are provided in Procedure 32 on Page 271.
13. Connect the DC power cable to the CMMmicro.
14. Plug the DC converter into an AC receptacle.

========== **end of procedure** ==========

19.6.6 Verifying CMMmicro Connections

To verify the CMMmicro connections after the APs and or BHs have been installed, perform the following steps.

Procedure 31: Verifying CMMmicro Connections

1. Access the web-based interface for each AP or BH by opening http://<ip-address>, where the <*ip-address*> is the address of the individual module.
2. In the Status page, verify that the time is expressed in GMT.
3. In the menu on the left-hand side of the web page, click on **GPS Status**.
4. Verify that the AP or BH is seeing and tracking satellites. (To generate the timing pulse, the module must track at least 4 satellites.)

========== **end of procedure** ==========

19.7 INSTALLING AN SM

To install the Canopy SM, perform the following steps:

Procedure 32: Installing the SM

1. Choose the best mounting location for your particular application.
2. Select the type of mounting hardware appropriate for this location.
3. Remove the base cover of the SM. (See Figure 47 on Page 132.)
4. In the powered down state, attach the cables to the SM. (See Procedure 8 on Page 143 and Figure 106 on Page 272.)
5. Optionally, attach the SM to the arm of the Canopy Passive Reflector dish assembly as shown in Figure 105.

RECOMMENDATION:
The arm is molded to receive and properly aim the module relative to the aim of the dish. Use stainless steel hose clamps for the attachment.

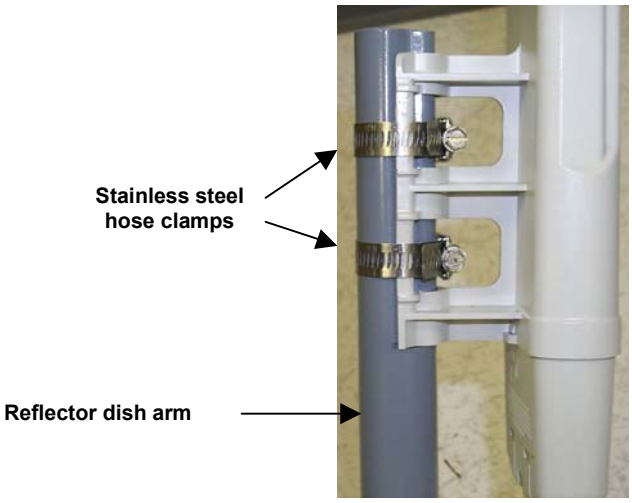


Figure 105: SM attachment to reflector arm

6. Use stainless steel hose clamps or equivalent fasteners to lock the SM into position.

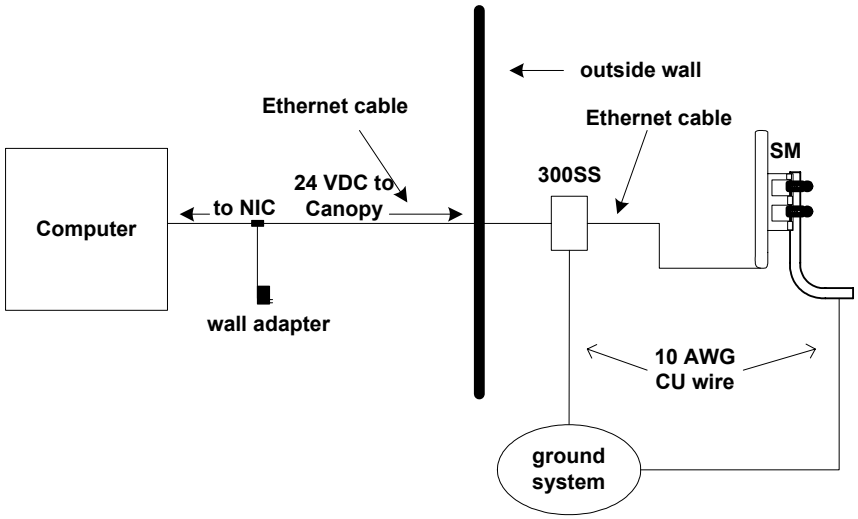


Figure 106: SM and computer wiring

7. Remove the cover of the 300SS Surge Suppressor.
8. With the cable openings facing downward, mount the 300SS to the *outside* of the subscriber premises.
9. Using diagonal cutters or long nose pliers, remove the knockouts that cover the cable openings to the 300SS.
10. Connect an Ethernet cable from the pig tail power adapter to either RJ-45 port of the 300SS.
11. Connect another Ethernet cable from the other RJ-45 port of the 300SS to the Ethernet port of the SM.
12. Wrap an AWG 10 (or 6mm^2) copper wire around the Ground post of the 300SS.
13. Tighten the Ground post locking nut in the 300SS onto the copper wire.

14. Securely connect the copper wire to the grounding system (Protective Earth) according to applicable regulations.
15. Connect a ground wire to the 300SS.
16. Replace the cover of the 300SS surge suppressor.
17. Connect the pig tail to the Ethernet/Power port on the computer.
    NOTE: When power is applied to a Canopy module or the unit is reset on the web-based interface, the module requires approximately 25 seconds to boot. During this interval, self-tests and other diagnostics are being performed. See Table 36 on Page 133.
18. Unlock the module from the locked down state.
19. On the computer, access the Alignment page of this module.
20. In the **RF Carrier Frequency** field, select the frequency that the AP transmits.
21. In the **RSSI Only Mode** field, ensure that the **Disabled** button is selected.
22. For coarse alignment of the SM, either
    a. use the LEDs in the module as follows:

       On the computer, click **Enable Aiming Mode**.
       NOTE: This places the module into the Normal Aiming Mode. The module is automatically placed into the Operating Mode after 15 minutes. To return the module to the Operating Mode before this interval has expired, click **Disable Aiming Mode**. To return the module to an aiming mode after this interval has expired, click **Enable Aiming Mode**.

       At the module, observe the six status LEDs in the module. See Figure 47 on Page 132.

       Move the module slightly in the vertical plane until the largest number of LEDs is lit.

    b. use the Audible Alignment Tone feature (Release 4.0 and later) as follows:

       On the computer, click **Disable Aiming Mode**.

       Connect the cable to the RJ-11 port of the SM.

       Connect the Alignment Tool Headset, an earpiece, or a small battery-powered speaker to this cable.

       Listen to the alignment tone for

       - pitch, which indicates greater RSSI by higher pitch.
       - volume, which indicates less jitter by higher volume.

       In Adobe Reader® 6.0 or later release, to hear an example of the alignment tone as the SM aligns and registers, click on the picture in Figure 107.

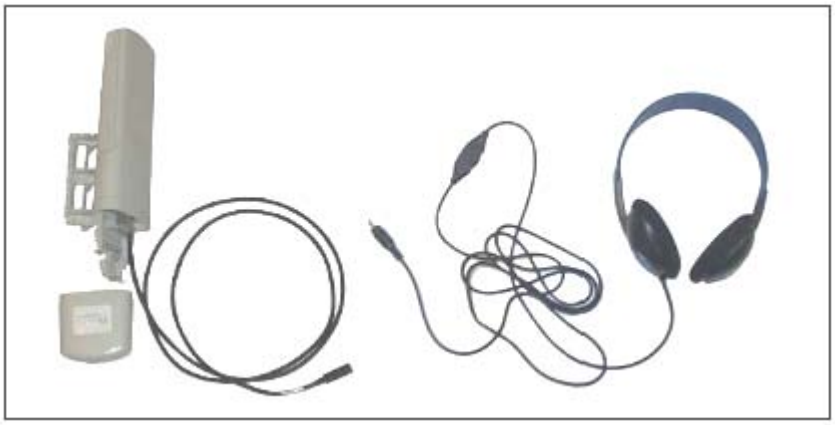


Figure 107: Audible Alignment Tone kit and example tone

Move the module slightly until you hear the highest pitch and highest volume.

Continue to move the module slightly until you hear the tone interruptions, if possible.

24. On the computer, in the **RSSI Only Mode** field, click **Enabled**.
25. Click **Enable Aiming Mode**.
26. Simultaneously, begin to
    - move the module slightly in the vertical plane.
    - on the computer, click **Enable Aiming Mode** frequently to refresh the page as the module moves (or select the auto-refresh option for this web page).
    - monitor the screen for a simultaneous RSSI level of greater than 700, jitter value between 0 and 4 in Release 4.0 and later releases or between 5 and 9 in any earlier release, and efficiencies greater than 90% for both the uplink and the downlink.
27. When the RSSI level is greater than 700, stop the movement of the module and click **Disable** in the **RSSI Only Mode** field.
28. Access the Status page.
29. Monitor this page for the messages Scanning, Syncing, Registering, Registered, Alignment.
    NOTE: If the SM does not register with the AP, ensure that both modules are configured to the same color code in the Configuration page of each. In Release 4.0 and later releases, the Expanded Stats page of the AP provides a link to the Reg Failed SMs page, where the cause of a registration failure may be found.
30. Resume slight movements of the module
31. When the best achievable values are simultaneously displayed on the Status page, lock the module into position.
    NOTE: If any of these values is not achieved, the SM may be operational but manifest occasional problems.

========== **end of procedure** ==========

19.8 VERIFYING AN AP-SM LINK

To verify the AP-SM link after the SM has been installed, perform the following steps.

Procedure 33: Verifying system performance

1. Access the web-based interface for the AP (by opening http://<*ip-address*>, where <*ip-address*> is the address of the individual module).
2. In the menu on the left-hand side of the web page, click on **GPS Status**.
3. Verify in the **Satellites Tracked** field that the AP is seeing and tracking satellites. (To generate the timing pulse, the module must track at least 4 satellites.)
4. Verify that the **Antenna Status** field displays the value OK.
5. Access the Status Page of the SM.
6. Verify that the SM is still registered to the AP.
7. Access the Configuration page of the SM.
8. Note the frequency that is selected in the **Custom RF Frequency Scan Selection List** field.
9. Access the Configuration page of the AP.
10. Verify that the frequency that is selected in the **RF Frequency Carrier** field is the same as noted above.
11. Access the AP Eval Data page of the SM.
12. Verify that the AP is shown in the **Sector ID** field.

========== **end of procedure** ==========

19.9 INSTALLING A REFLECTOR DISH

The internal patch antenna of the module illuminates the Canopy Passive Reflector Dish from an offset position. The module support tube provides the proper angle for this offset.

19.9.1 Both Modules Mounted at Same Elevation

For cases where you are mounting the other module in the link is mounted at the same elevation, fasten the *mounting hardware leg* of the support tube vertical for each module. When the hardware leg is in this position

- the reflector dish has an obvious downward tilt.
- the *module leg* of the support tube *is not* vertical.

For a mount to a non-vertical structure such as a tapered tower, use a plumb line to ensure that the hardware leg is vertical when fastened. Proper dish, tube, and module positions for a link in this case are illustrated in Figure 108.

Figure 108: Correct mount, with module support arm plumb behind reflector dish

Improper dish, tube, and module positions for this case are illustrated in Figure 109.

Figure 109: Incorrect mount, with module plumb in front of reflector dish

19.9.2 Modules Mounted at Different Elevations

For cases where the other module in the link is mounted at a different elevation, the assembly hardware allows tilt adjustment. The proper angle of tilt can be calculated as a factor of both the difference in elevation and the distance that the link spans. Even in this case, a plumb line and a protractor can be helpful to ensure the proper tilt. This tilt is typically minimal.

The number of degrees to offset (from vertical) the mounting hardware leg of the support tube is equal to the angle of elevation from the lower module to the higher module (b in the example provided in Figure 40 on Page 110).

19.9.3 Mounting Assembly

Both the hardware that Mounting Assembly 27RD provides for adjustment and the relationship between the offset angle of the module and the direction of the beam are illustrated in Figure 110.

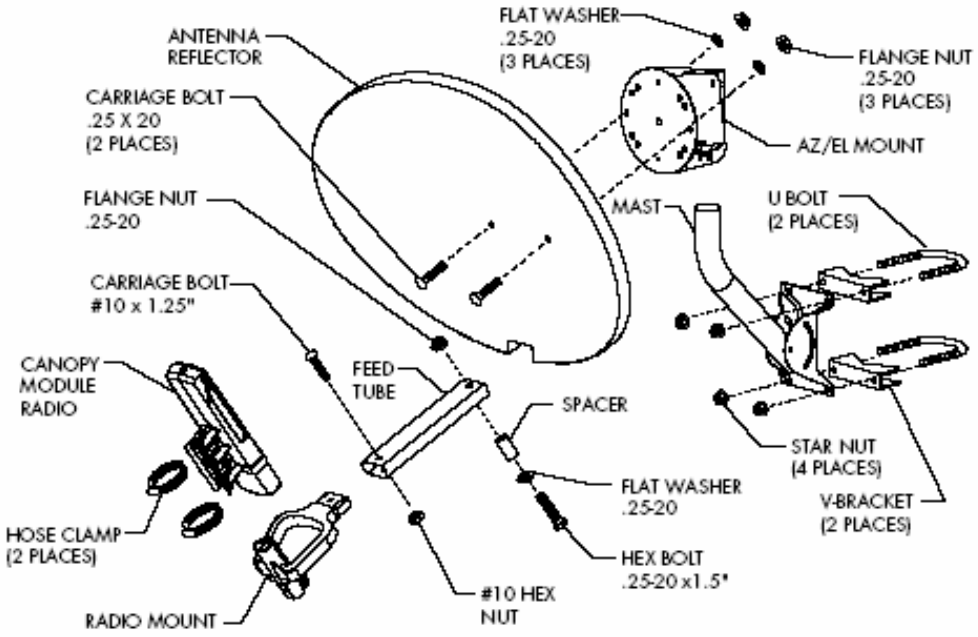


Figure 110: Mounting assembly, exploded view

19.10 INSTALLING A BH TIMING MASTER

To install the Canopy BHM, perform the following steps:

Procedure 34: Installing the BHM

1. If this is a 20-Mbps BH, set the **Modulation Scheme** parameter in the Configuration web page of the BHM to 10 Mbps (for easier course aiming).
2. Remove power from the BHM.
3. Choose the best mounting location for your particular application.
4. Optionally, attach the BHM to the arm of the Canopy Passive Reflector dish assembly as shown in Figure 111.

RECOMMENDATION:
The arm is molded to receive and properly aim the module relative to the aim of the dish. Stainless steel hose clamps should be used for the attachment.

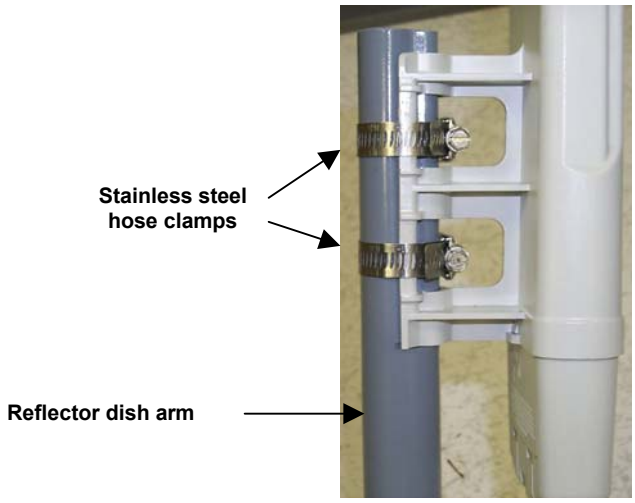


Figure 111: BH attachment to reflector arm

5. Align the BHM as follows:
   a. Move the module to where the link will be unobstructed by the radio horizon and no objects penetrate the Fresnel zone. (The Canopy System Calculator page AntennaElevationCalcPage.xls automatically calculates the minimum antenna elevation that is required to extend the radio horizon to the other end of the link. The Canopy System Calculator page FresnelZoneCalcPage.xls automatically calculates the Fresnel zone clearance that is required between the visual line of sight and the top of a high-elevation object.)
   b. Use a local map, compass, and/or GPS device as needed to determine the direction to the BHS.
   c. Apply the appropriate degree of downward or upward tilt. (The Canopy System Calculator page DowntiltCalcPage.xls automatically calculates the angle of antenna downward tilt that is required.)
   d. Ensure that the BHS is within the beam coverage area. (The Canopy System Calculator page BeamwidthRadiiCalcPage.xls automatically calculates the radii of the beam coverage area.)
6. Using stainless steel hose clamps or equivalent fasteners, lock the BHM into position.
7. Remove the base cover of the BHM. (See Figure 47 on Page 132.)
8. If this BHM *will not* be connected to a CMMmicro, optionally connect a utility cable to a GPS timing source and then to the RJ-11 port of the BHM.
9. Either connect the BHM to the CMM or connect the DC power converter to the BHM and then to an AC power source.
   RESULT: When power is applied to a Canopy module or the unit is reset on the web-based interface, the module requires approximately 25 seconds to boot. During this interval, self-tests and other diagnostics are being performed.
10. Access the Configuration page of this module.

11. Set the **Sync Input** parameter to the **Sync to Received Signal (Power Port)** selection.

end of procedure

19.11 INSTALLING A BH TIMING SLAVE

To install the Canopy BHS, perform the following steps:

Procedure 35: Installing the BHS

1. If this is a 20-Mbps BH, set the **Modulation Scheme** parameter in the Configuration web page of the BHM to 10 Mbps (for easier course aiming).
2. Remove power from the BHS.
3. Choose the best mounting location for your particular application.
4. Optionally, attach the BHS to the arm of the Canopy Passive Reflector dish assembly as shown in Figure 111.

RECOMMENDATION:
The arm is molded to receive and properly aim the module relative to the aim of the dish. Stainless steel hose clamps should be used for the attachment.

5. Align the BHS as follows:
   a. Move the module to where the link will be unobstructed by the radio horizon and no objects penetrate the Fresnel zone. (The Canopy System Calculator page AntennaElevationCalcPage.xls automatically calculates the minimum antenna elevation that is required to extend the radio horizon to the other end of the link. The Canopy System Calculator page FresnelZoneCalcPage.xls automatically calculates the Fresnel zone clearance that is required between the visual line of sight and the top of a high-elevation object.)
   b. Use a local map, compass, and/or GPS device as needed to determine the direction to the BHS.
   c. Apply the appropriate degree of downward or upward tilt. (The Canopy System Calculator page DowntiltCalcPage.xls automatically calculates the angle of antenna downward tilt that is required.)
6. Using stainless steel hose clamps or equivalent fasteners, lock the BHS into position.
7. Remove the base cover of the BHS. (See Figure 47 on Page 132.)
8. Connect the DC power converter to the BHM and then to an AC power source. ***RESULT:*** When power is applied to a Canopy module or the unit is reset on the web-based interface, the module requires approximately 25 seconds to boot. During this interval, self-tests and other diagnostics are being performed.
9. Connect the module to an Ethernet port on a computing device.

10. On the computing device, access the Alignment page of this module. An example of the Alignment screen is displayed in Figure 112.

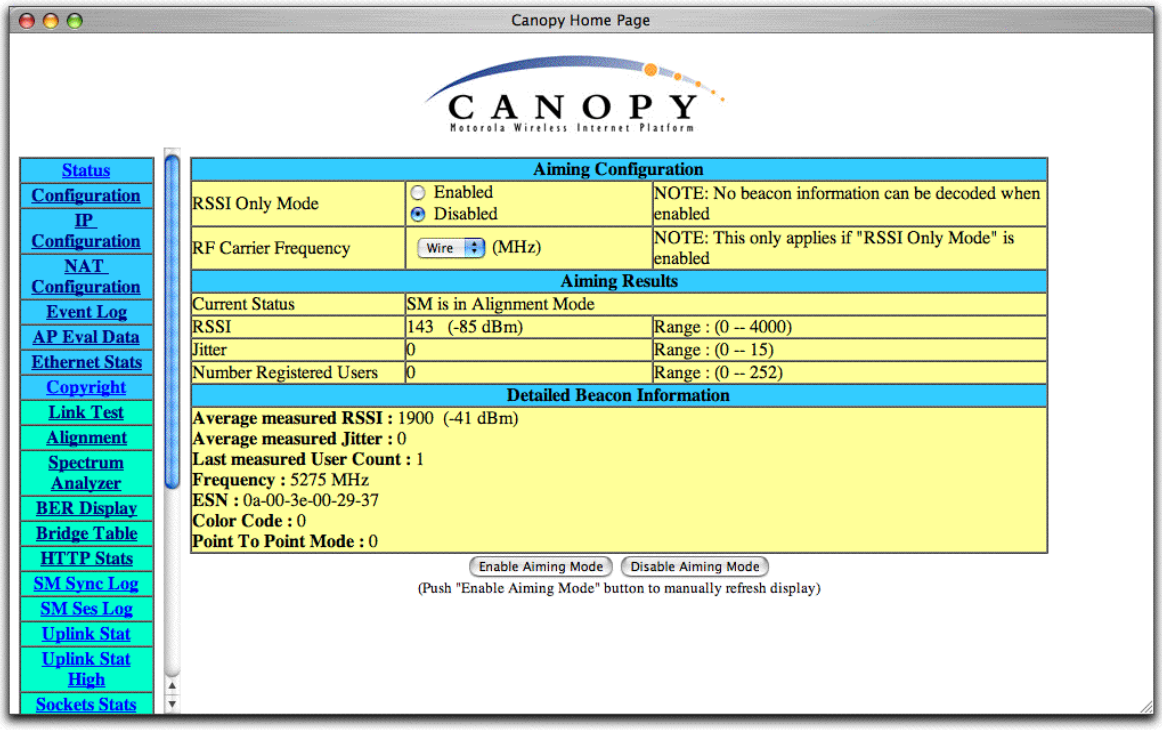


Figure 112: Alignment screen

11. In the **RF Carrier Frequency** field, select the frequency that the BHM transmits.
12. In the **RSSI Only Mode** field, ensure that the **Disabled** button is selected.
13. To use the LEDs for coarse alignment: (instead of the Audible Alignment Tone feature), perform the following steps:
    a. On the computer, click **Enable Aiming Mode**.
    NOTE: This places the module into the Normal Aiming Mode. The module is automatically placed into the Operating Mode after 15 minutes. To return the module to the Operating Mode before this interval has expired, click **Disable Aiming Mode**. To return the module to an aiming mode after this interval has expired, click **Enable Aiming Mode**.
    b. At the module, observe the six status LEDs in the module. See Figure 47 on Page 132.
    c. Move the module slightly in the vertical plane until the largest number of LEDs is lit.
14. To use the Audible Alignment Tone feature for coarse alignment (in Release 4.0 and later), perform the following steps:
    a. On the computer, click **Disable Aiming Mode**.
    b. Connect the cable to the RJ-11 port of the SM.

c. Connect the Alignment Tool Headset, an earpiece, or a small battery-powered speaker to this cable.

d. Listen to the alignment tone for

- pitch, which indicates greater RSSI by higher pitch.
- volume, which indicates less jitter by higher volume.

In Adobe Reader® 6.0 or later release, to hear an example of the alignment tone as the SM aligns and registers, click on the picture in Figure 113.

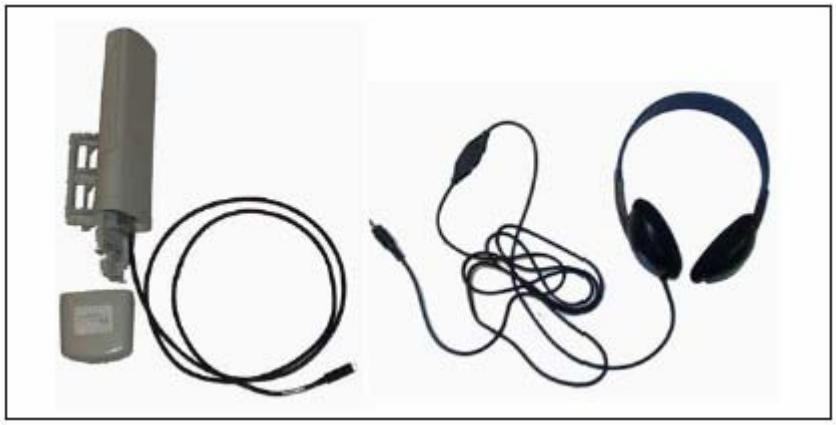


Figure 113: Audible Alignment Tone kit and example tone

e. Move the module slightly until you hear the highest pitch and highest volume.

f. Continue to move the module slightly until you hear the tone interruptions, if possible.

15. On the computing device, in the **RSSI Only Mode** field, click **Enabled**.
16. Click **Enable Aiming Mode**.
17. Simultaneously, begin to
    - move the module slightly in the vertical plane.
    - on the computer, click **Enable Aiming Mode** frequently to refresh the page as the module moves (or select the auto-refresh option for this web page).
    - monitor the screen for a simultaneous RSSI level of greater than 700, jitter value between 0 and 4 in a 10-Mbps BH in Release 4.0 and later releases, between 0 and 9 in a 20-Mbps BH, or between 5 and 9 in any earlier release, and efficiencies greater than 90% for both the uplink and the downlink.
18. When the RSSI level is greater than 700, stop the movement of the module and click **Disable** in the **RSSI Only Mode** field.
19. If this link will be a 20-Mbps BH link, set the **Modulation Scheme** parameter in the Configuration web page of both the BH timing master and the BH timing slave to 20 Mbps (for fine aiming and continued operation).
20. Access the Status page.
21. Monitor this page for the messages **Scanning**, **Syncing**, **Registering**, **Registered**, and **Alignment**.

NOTE: If the BH timing slave does not register with the BH timing master, ensure that both modules are configured to the same color code in the Configuration page of each.

22. Resume slight movements of the module
23. When the best achievable values are simultaneously displayed on the Status page, lock the module into position.
    NOTE: If any of these values is not achieved, the BH timing slave may be operational but manifest occasional problems.

========== **end of procedure** ==========

19.12 UPGRADING A BH LINK TO BH20

To replace a pair of 10-Mbps BHs with 20-Mbps BHs, you can minimize downtime by temporarily using the 10-Mbps capability in the faster modules. However, both interference and differences in receiver sensitivity can make alignment and link maintenance more difficult than in the previous 10-Mbps link. The effects of these factors are greater at greater link distances, particularly at 5 miles or more.

Especially in shorter spans, these factors may not be prohibitive. For these cases, set the first replacement module to 10-Mbps and establish the link to the 10-Mbps BH on the far end. Similarly, set the second replacement module to 10-Mbps and re-establish the link. With both of the faster modules in place and with an operational link having been achieved, reset their modulation rates to 20 Mbps.

19.13 VERIFYING A BH LINK

To verify the performance of the BH link after the BHs have been installed, perform the following steps.

Procedure 36: Verifying performance for a BH link

1. Access the web-based interface for the BHM (by opening http://<ip-address>, where <*ip-address*> is the address of the individual module).
2. Verify that the **Antenna Status** field displays the value OK.
3. Access the Status Page of the BHS.
4. Verify that the BHS is still registered to the BHM.
5. Access the AP Eval Data page of the BHS.
6. Verify that the BH timing master is shown in the **Sector ID** field.

========== **end of procedure** ==========

20 VERIFYING SYSTEM FUNCTIONALITY

To verify system functionality after the APs and or BHs have been installed, perform the following steps.

Procedure 37: Verifying System Functionality

1. For each installed AP, use a computer connected to an SM set to a compatible configuration (frequency and color code, for example) and verify link functionality.
2. For each BH installed, use a notebook computer connected to a BH (BHM or BHS, as appropriate) set to a compatible configuration and verify link functionality.
3. If a network data feed is present and operational, use an SM or BHS to verify network functionality.

end of procedure

MANAGING YOUR CANOPY NETWORK

21 GROWING YOUR NETWORK

Keys to successfully growing your network include

- monitoring the RF environment.
- considering software release compatibility.
- redeploying modules appropriately and quickly.

21.1 MONITORING THE RF ENVIRONMENT

Regardless of whether you are maintaining or growing your network, you may encounter new RF traffic that can interfere with your current or planned equipment. Regularly measuring *over a period of time* and logging the RF environment, as you did before you installed your first equipment in an area, enables you to recognize and react to changes.

21.1.1 Spectrum Analyzer Web Pages

IMPORTANT!

The following sections describe the use of a Canopy module in scan mode to analyze the RF spectrum. While a module is in the scan mode, no RF connectivity to that module is possible until either you click **Disable** on the Spectrum Analyzer page or 15 minutes elapses since the module entered the scan mode.

For this reason

- *do not* enable the spectrum analyzer from an RF-connected module. (No readings will be displayed when the RF connection is re-established.)
- be advised that, if you enable the spectrum analyzer by Ethernet connection, any current RF connection to that module drops.

You can use any SM or BHS in Release 4.1.n or later, or any AP in Release 6.1 or later, to see at once the frequency and power level of any detectable signal that is within, above, or below the frequency band range of the module.

RECOMMENDATION:

Vary the days and times when you analyze the spectrum in an area. The RF environment can change throughout the day or throughout the week.

Temporarily deploy an SM or BHS for *each* frequency band range that you need to monitor and Access the Spectrum Analyzer web page of the module. (For access from a PDA, see PDA Access to Canopy Modules on Page 257.) To enter the scan mode and view readings, click **Enable**. A Canopy SM/BHS displays the Spectrum Analyzer web page as either a graphical or a tabular page. The differences between these page types are shown in Table 45.

Table 45: Differences between graphical and tabular Spectrum Analyzer page

Graphical Spectrum Analyzer Page	Tabular Spectrum Analyzer Page
Green bars display the latest readings.	Table data provide the latest readings.
A yellow tick indicates the highest reading since the SM entered the scan mode.	Only readings from the latest page refresh are provided.
A red tick indicates any −4 dBm reading.	No indication is provided for high readings.

21.1.2 Graphical Spectrum Analyzer Display

An SM/BHS displays the graphical spectrum analyzer only if both

- the module operates on Release 4.2 or a later release.
- the module is calibrated for received power. This is the case only if the Status page reports received power in units of both RSSI and dBm. More recent modules are calibrated before shipment.

An example of the graphical Spectrum Analyzer web page is shown in Figure 114.

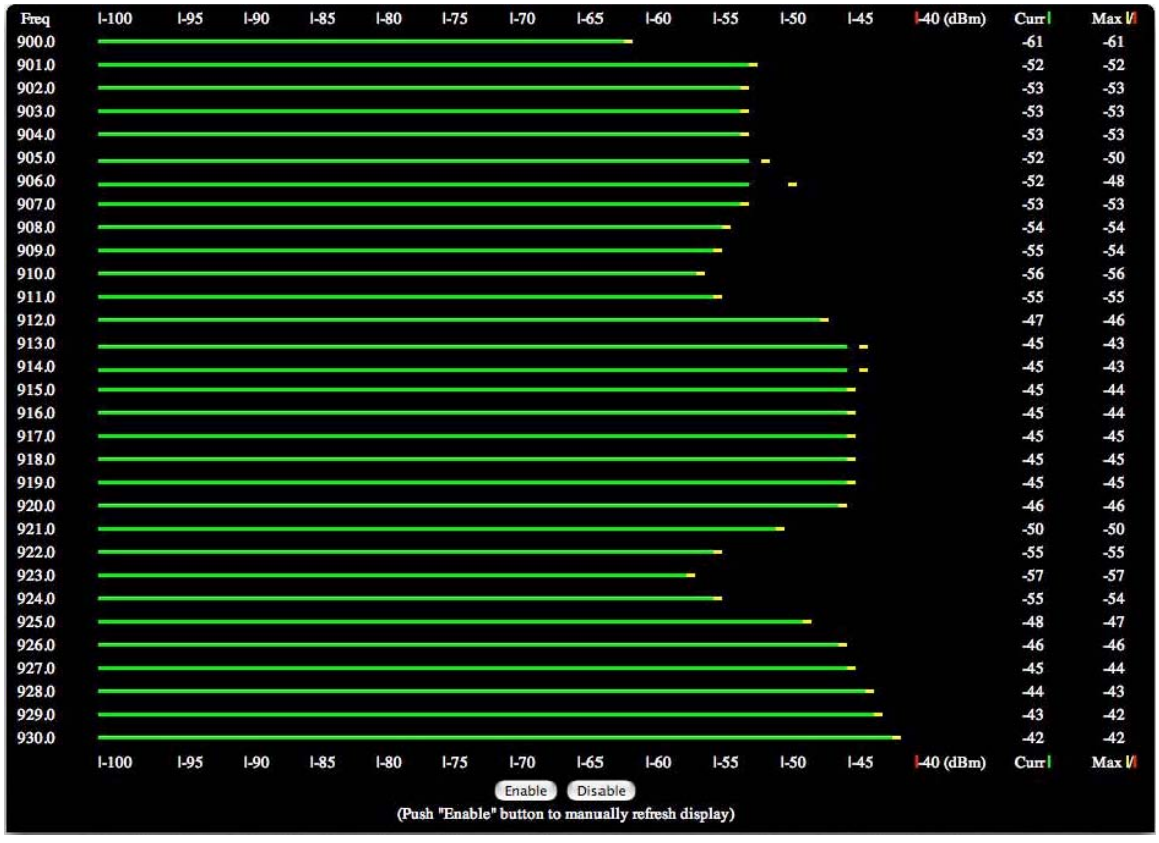


Figure 114: Spectrum Analyzer screen, 900-MHz SM

Colors in the display have the following meanings:

- Green bars show the most recent measurements.
- Yellow ticks show the maximum measurements from the current spectrum analysis session.
- Red ticks show measurements of −40 dBm or stronger.

21.1.3 Tabular Spectrum Analyzer Display

An SM/BHS displays the tabular spectrum analyzer if either

- the module operates on a Canopy system release that is earlier than Release 4.2.
- the module *is not* calibrated for received power. This is the case if the Status page reports received power in units of only RSSI. Earlier modules *were not* calibrated as shipped.

You can calibrate an uncalibrated module. If you wish to do so (in lieu of continuing with the tabular Spectrum Analyzer page), download the required instructions and data from http://www.canopywireless.com/calibrate.php.

NOTE:
Although calibration improves the measurement of received power, calibration has no effect on reception, transmission, or other aspects of performance.

An example of the tabular Spectrum Analyzer web page is shown in Figure 115.

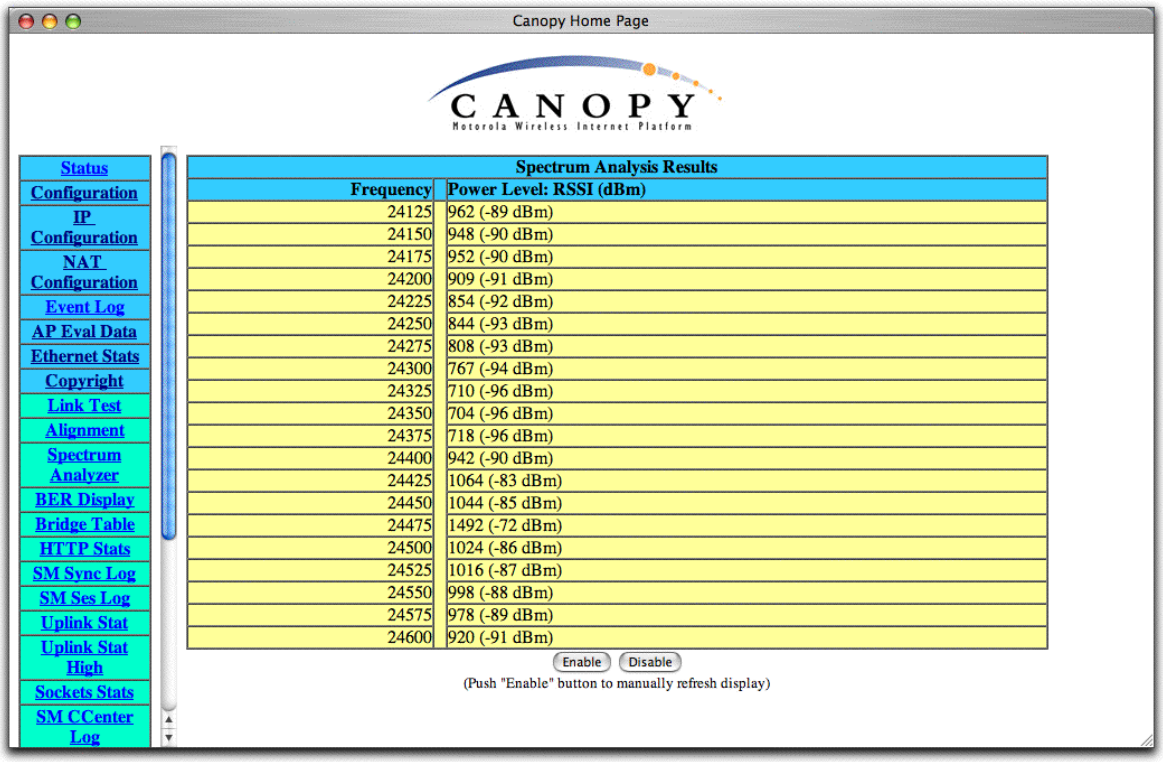


Figure 115: Spectrum Analyzer screen, 2.4-GHz SM

21.1.4 Updating the Spectrum Analyzer Page Readings

To keep the displayed data current, either set this page to automatically refresh or repeatedly click the **Enable** button. When you are finished analyzing the spectrum, click the **Disable** button to return the module to normal operation.

21.1.5 Using the AP as a Spectrum Analyzer

In Canopy System Release 6.1 and later, you can temporarily transform an AP into an SM and thereby use the spectrum analyzer functionality. This is the only purpose supported for the transformation.

CAUTION!

Although you can toggle the AP **Device Type** parameter to **SM** in the over-the-air interface, you lose connectivity to the AP during spectrum analysis and can regain connectivity (and toggle it back to AP) through only the wired Ethernet interface to the AP. For this reason, you should perform the transformation to SM in the Ethernet interface.

To transform the AP into an SM for spectrum analysis and return the device to an AP, perform the following steps.

Procedure 38: Using the Spectrum Analyzer in AP feature

1. Connect to the wired Ethernet interface of the AP.
2. Access the Configuration page of the AP.
3. Set the **Device Type** parameter to **SM**.
4. Click **Save Changes**.
5. Click **Reboot**.
6. When the module has rebooted as an SM, click the Expanded Stats navigation link.
7. Click the Spectrum Analyzer navigation link.
8. Either set this page to automatically refresh or repeatedly click the **Enable** button.
   RESULT: The SM enters the scan mode.
9. When you are finished analyzing the spectrum, click the **Disable** button.
10. Access the Configuration page of the SM.
11. Set the **Device Type** parameter to **AP**.
12. Click **Save Changes**.
13. Click **Reboot**.
    RESULT: The AP boots with its previous frequency setting.

21.2 CONSIDERING SOFTWARE RELEASE COMPATIBILITY

Within the same Canopy network, modules can operate on Releases 4.n.n, and 6.n.n. However, the features that can be enabled are limited to those that the earliest software supports.

21.2.1 Designations for Hardware and Firmware

Canopy documentation refers to both FPGAs and hardware series (for example, Hardware Series P7). P9 provides advanced capabilities. For this reason, the documentation in some instances refers specifically to P9 as being required for a feature. The correlation between hardware series and the MAC addresses of the radio modules is provided in Table 46.

Table 46: Hardware series by MAC address

Radio Frequency Band Range	Hardware Series	
	P7 or P8 in These MAC Addresses	P9 or Later in These MAC Addresses
900	None	All
2.4	≤ 0A003E20672B	≥ 0A003E20672C
5.2	≤ 0A003E00F4E3	≥ 0A003E00F4E4
5.4	None	All
5.7	≤ 0A003EF12AFE	≥ 0A003EF12AFF

The correlation between FPGA dates and CANOPYBOOT versions is provided in Table 47.

Table 47: FPGA and CANOPYBOOT versions

Rel	Hardware Series P7 or P8				Hardware Series P9				Boot Version (block.bin)
	SW Scheduler		HW Scheduler		SW Scheduler		HW Scheduler		
	DES	AES	DES	AES	DES	AES	DES	AES	
3.1.5	091102								1.0
4.0	042903	041403							1.1
4.0.1	042903	041403							1.1
4.0.2	062403	041403							1.1
4.0.4	062403	041403							1.1
4.1	062403	041403							1.1
4.1.3	062403	041403							2.3
4.2.1	062403	041403							2.5
4.2.2					051804				3.0
4.2.3	062403	041403			071904	071904			3.0
4.2.7	051104	051104			082504	082504			3.0
6.0					092904		092904		3.0
6.1	051104	051104	110204		111504	111504	111604	111604	3.0

21.2.2 Application, Boot, and FPGA Software Upgrades

Within a module, compatibility is essential between the application, FPGA, and boot software versions. A direct upgrade across more than one progressive software release is possible in some instances. All instances in which a direct upgrade is possible are shown in Table 48.

Table 48: Upgradability from previous software releases

A module can be directly upgraded[1] from…			to…		
System Release	**with FPGA Version**	**and Boot Version**	**System Release**	**with FPGA Version**	**and Boot Version[2]**
Nahum (SP3)	121401a7	1.0	3.2.5	091102xx	1.0
	091102xx[3]	1.0			
3.n.n	121401a7	1.0	4.2.3	091102xx	1.0
	091102xx	1.0			
4.0.n[4]	062403xx	1.1	4.2.3	062403xx (DES) 041403xx (AES)	2.7
4.1.n	062403xx	1.1	6.1[6]	[various]	3.0
4.2.3	062403xx (DES) 041403xx (AES)	2.7			
4.2.7	051104xx	3.0			
4.2.7	082504xx	3.0			
6.0[5]	092904xx	3.0			

NOTES:

1. An upgrade to a particular release may require a unique procedural sequence that depends on what release the module is being upgraded from.

2. **Before an upgrade of system release or FPGA version in any module whose boot block is Version 2.5, you *must* upgrade the boot block to Version 2.7.**

3. xx indicates any two characters.

4. ***Do not* use the SM Auto-update feature (manually or with the Canopy Network Updater Tool [CNUT]) to upgrade from Release 4.0.n to Release 4.2. CNUT and SM Auto-update require Release 4.1 or later.**

5. This system release is dedicated to only the 900-MHz AP and SM.

6. Upgrade to Release 6.1 requires CNUT.

21.2.3 System Release 6.1 Compatibility

If you deploy Canopy System Release 6.1, observe the following caveats:

- If you implement VLAN
  - first upgrade the AP and all SMs in the sector to Release 6.1.
  - you do not require VLAN-aware end stations (the SMs are VLAN aware), but you likely require a VLAN switch in your network.

- To implement both VLAN and per-SM MIR, you can
  - select the SM as the source for MIR/CIR/VLAN settings and set the MIR in each SM (BAM Release 2.0 *cannot* do this).
  - select the AP as the source for MIR/CIR/VLAN settings and set the MIR in the AP (for all SMs in the sector, except those in which MIR has been set).
- If you modify any range, downlink percentage, or slot parameter in an AP (or BHM) that operates on Release 6.1, and then experience trouble connecting to an SM (or BHS) that operates on an earlier release, attempt the following remedy in the AP (or BHM):
  1. At the bottom of the Configuration web page, click **Adjust Frame for All**.
  2. If **Reboot Required** appears in red near the **Reboot** button, click **Reboot**.
- Where you deploy an Advantage AP that is set for Hardware Scheduler, observe the following precautions:
  - Ensure that all SMs that will link to the AP are set for Hardware Scheduler (the AP cannot communicate with any SM that runs the Software Scheduler—the default controller of the interface).
  - Use *only* the Canopy Network Updater Tool (CNUT) to enable Hardware Scheduler on the SMs.
  - Ensure that each SM that will use the high-priority channel is Series P9 or later. (See Table 46 on Page 289.)
- In any 900-MHz AP that meets *either* of the following conditions, select **Disable** for the **6.0 Compatibility** parameter:
  - range set to greater than 40 miles.
  - downlink percentage set to greater than 80%.

21.2.4 BAM Software Compatibility

Bandwidth and Authentication Manager (BAM) software acts independent of the application, FPGA, and boot software version. BAM Release 1.1 and later releases are sensitive to the configurable parameters of a module regardless of changes in parameter names through evolving system software releases. For example, the **Authorization Key** parameter name has been changed to **Authentication Key**. This change does not affect whether BAM software can read the key.

The compatibility of BAM software, Red Hat Linux operating system, and Canopy system software releases is indicated in Table 49.

Table 49: Compatibility of software releases

BAM	Red Hat Linux OS	Canopy System
1.0	7.3	3.1.x
1.1	9 or Enterprise Version 3 (WS or ES)	3.1.x through 4.2
2.0	Enterprise Version 3 (WS or ES)	4.x through 6.x
2.1	Enterprise Version 3 (WS or ES)	7.1 and later

21.2.5 CMMmicro Software and Hardware Compatibility

The CMMmicro contains both a programmable logic device (PLD) and software. These must be compatible. The PLD that is compatible with CMMmicro Release 2.0.8 is PLD 5.

Further, the CMMmicro must be compatible with both the application software release and the hardware of attached APs and BHs. These attached modules must

- be operating on Release 4.0 or a later release.
- have been manufactured in October 2002 or later.

APs and BHs that were manufactured earlier do not support sync on the power leads of the Ethernet port. To determine whether the AP or BH hardware is compatible with the CMMmicro, see Table 50.

Table 50: AP/BH compatibility with CMMmicro

Frequency Band Range	Range of MAC Addresses (ESNs)	
	Incompatible with CMMmicro	Compatible with CMMmicro
900 MHz AP	none	all
2.4 GHz	none	all
5.2 GHz	≤ 0A003E0021C8	≥ 0A003E0021C9
5.7 GHz	≤ 0A003EF00F79	≥ 0A003EF00F7A

21.2.6 MIB File Set Compatibility

Although MIB files are text files (not software), they define objects associated with configurable parameters and indicators for the module and its links. In each release, some of these parameters and indicators are not carried forward from the previous release, and some parameters and indicators are introduced or changed.

For this reason, use the MIB files from your download to replace previous MIB files in conjunction with your software upgrades, even if the file names are identical to those of your previous files. Date stamps on the MIB files distinguish the later set.

21.3 REDEPLOYING MODULES

Successfully redeploying a module may involve

- maintaining full and accurate records of modules being redeployed from warehouse stock.
- exercising caution about
  - software compatibility. For example, whether desired features can be enabled with the redeployed module in the network.
  - procedural handling of the module. For example
    - whether to align the SM or BHS by RSSI and jitter or by only jitter.
    - whether the module auto-senses the Ethernet cable connector scheme.

- hardware compatibility. For example, where a CMMmicro is deployed.
- the value of each configurable parameter. Whether all are compatible in the new destination.

◦ remembering to add the redeployed SM to the ESN data table in the BAM server(s).

21.3.1 Wiring to Extend Network Sync

The following procedure can be used to extend network sync by one additional hop, as described under Passing Sync in an Additional Hop on Page 70. Where a collocated module receives sync over the air, the collocated modules can be wired to pass the sync as follows:

Procedure 39: Extending network sync

1. Connect the GPS Utility ports of the collocated modules using a sync cable with RJ-11 connectors.
2. Set the **Sync Input** parameter on the Configuration page of the collocated AP or BH timing master to **Sync to Received Signal (Timing Port)**.
3. Set the **Frame Timing Pulse Gated** parameter on the Configuration page of the collocated SM or BH timing slave to **Enable**.
   NOTE: This setting prevents interference in the event that the SM or BH timing slave loses sync.

end of procedure

22 SECURING YOUR NETWORK

22.1 ISOLATING APS FROM THE INTERNET

Ensure that the IP addresses of the APs in your network

- are not routable over the Internet.
- do not share the subnet of the IP address of your user.

RFC 1597, *Address Allocation for Private Subnets*, reserves for private IP networks three blocks of IP addresses that are not routable over the Internet:

- Class A has one reserved network, 10.0.0.0 to 10.255.255.255.
- Class B has 16 reserved networks, 172.16.0.0 to 172.31.255.255.
- Class C has 256 reserved networks, 192.168.0.0 to 192.168.255.255.

An example of a securely configured private IP network is displayed in Figure 116.

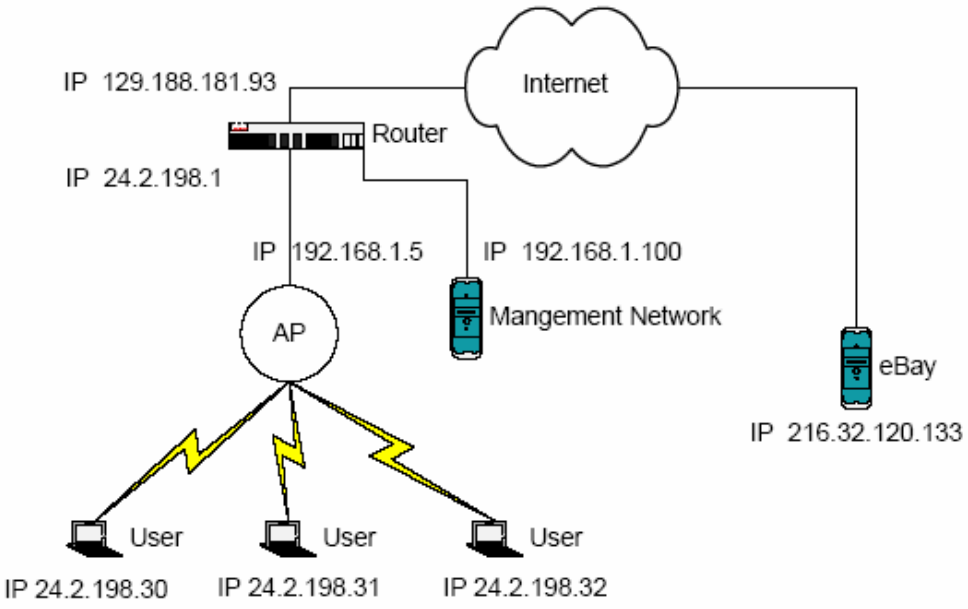


Figure 116: Example of private IP network

22.2 ENCRYPTING CANOPY RADIO TRANSMISSIONS

Canopy systems employ the following forms of encryption for security of the wireless link:

- BRAID–a security scheme that the cellular industry uses to authenticate wireless devices.
- DES–Data Encryption Standard, an over-the-air link option that uses secret 56-bit keys and 8 parity bits.
- AES–Advanced Encryption Standard, an extra-cost over-the-air link option that provides extremely secure wireless connections. AES uses 128-bit secret keys as directed by the government of the U.S.A. AES is not exportable and requires a special AP to process the large keys.

BRAID

BRAID is a stream cipher that the TIA (Telecommunications Industry Association) has standardized. Standard Canopy APs and SMs use BRAID encryption to

- calculate the per-session encryption key (independently) on each end of a link.
- provide the digital signature for authentication challenges.

DES Encryption

Standard Canopy modules provide DES encryption. DES performs a series of bit permutations, substitutions, and recombination operations on blocks of data. DES Encryption does not affect the performance or throughput of the system.

AES Encryption

Motorola also offers Canopy products that provide AES encryption. AES uses the Rijndael algorithm and 128-bit keys to establish a higher level of security than DES. Because of this higher level of security, the government of the U.S.A. controls the export of communications products that use AES (among which the Canopy AES feature activation key is one) to ensure that these products are available in only certain regions and by special permit.

The Canopy distributor or reseller can advise service providers about current regional availability. Canopy AES products are certified as compliant with the Federal Information Processing Standards (FIPS) in the U.S.A. The National Institute of Standards and Technology (NIST) in the U.S.A. has specified AES for significantly greater security than that which DES provides. NIST selected the AES algorithm for providing the best combination of security, performance, efficiency, implementation, and flexibility. NIST collaborates with industry to develop and apply technology, measurements, and standards.

AES-DES Operability Comparisons

This section describes the similarities and differences between DES and AES products, and the extent to which they may interoperate.

Key Consistency

The DES AP and the DES BHM modules are factory-programmed to enable or disable *DES* encryption. Similarly, the AES AP and the AES BHM modules are factory-programmed to enable or disable *AES* encryption.

In either case, the authentication key entered in the Configuration page establishes the encryption key. For this reason, the authentication key must be the same on each end of the link. See Authentication Key on Page 212.

Feature Availability

Canopy AES products run the same software as DES products. Thus feature availability and functionality are and will continue to be the same, regardless of whether AES encryption is enabled. All interface screens are identical. However, when encryption is enabled on the Configuration screen

- the AES product provides AES encryption.
- the DES product provides DES encryption.

Field-programmable Gate Array

Canopy AES products and DES products use different FPGA (field-programmable gate array) loads. However, the AES FPGA will be upgraded as needed to provide new features or services similar to those available for DES products.

Signaling Rates for Backhaul Modules

DES BHs are available in both 10-Mbps and 20-Mbps signaling rates. AES BHs are available with only a 10-Mbps signaling rate.

Upgradeability

Canopy DES products cannot be upgraded to AES. To have the option of AES encryption, the service provider must purchase AES products.

Interoperability

Canopy AES products and DES products do not interoperate when enabled for encryption. For example, An AES AP with encryption enabled cannot communicate with DES SMs. Similarly, an AES Backhaul timing master module with encryption enabled cannot communicate with a DES Backhaul timing slave module.

However, if encryption is disabled, AES modules can communicate with DES modules.

22.3 MANAGING PASSWORD ACCESS

22.3.1 Configuring Display Only and Full Access Passwords

The **Display-Only Access** password protection interacts with the **Full Access** password protection as described in Table 51.

Table 51: Types of access per password combination

Configuration Page Passwords		FTP or telnet Requires[1]		Web Interface Requires		Web Interface Permissions	
Display-Only	**Full Access**	**User Name**	**Password**	**User Name**	**Password**	**Who Can View**	**Who Can Change**
unset	unset	none	none	none	none	anyone	anyone
set	unset	`root`	Display-Only Access[2]	none	Display-Only Access	Display-Only user	Display-Only user[2]
unset	set	`root`	Full Access[3]	none	Full Access	Full Access user	Full Access user
set	set	`root`	Full Access[3]	none	either	either user	Full Access user

NOTES:

1. The FTP and telnet interfaces permit whoever authenticates to view or change module data.
2. If you deploy a module with this password combination, ensure that your intent is to allow the Display-Only user to view or change module data.
3. If you deploy a module with either of these password combinations, the Display-Only user cannot authenticate in an FTP or telnet interface, even with the user name root and the set Display-Only Access password.

Because of these interactions, manage passwords for a module as follows:

- To allow anyone who can interface with a module to view or change module data, set *neither* password.
- To allow only one user to have access to a module, set *either* the Display-Only Access password or the Full Access password.
- To allow one user to have view-only access and another user to have both view and change access, set *both* passwords.

22.3.2 Setting and Changing Passwords

Setting and Changing Canopy Module Passwords

To set the **Display-Only Access** password, enter the same expression in both **Display-Only Access** fields for verification. When the web-based interface prompts for this password, no user name is required. However, when a `telnet` or FTP session prompts for this password, you must enter the user name **`root`** in addition to the password.

To set the **Full Access** password, enter the same expression in both **Full Access** fields for verification. When the web-based interface prompts for this password, no user name is required. However, when a `telnet` or FTP session prompts for this password, you must enter the user name **`root`** in addition to the password.

RECOMMENDATION:
Note the passwords that you enter. Ensure that you can readily associate these passwords both with the module and with the other data that you store about the module.

Good business practice is to maintain organized records for all IP addresses and passwords. Overriding these in a tower-mounted module requires both a tower climb and downtime for a portion of your network.

If you set and then forget either or both passwords, then you must both

1. physically access the module.
2. use an override plug to electronically access the module configuration parameters at 169.254.1.1. See Overriding Forgotten IP Addresses or Passwords on AP, SM, or BH on Page 302.

After any password is set and a reboot of the module has occurred, a **Password Set** indicator appears to the right of the field. You can unset either password (revert the access to no password required) as follows:

1. Authenticate yourself using the current password.
2. Access the Configuration web page of the module.
3. Type a space into the appropriate (**Display-Only Access** or **Full Access**) field.
4. Type a space into the redundant verification field.
5. Click **Save Changes**.
6. Click **Reboot**.

Setting and Changing BAM SSE Passwords

Distinctive fonts indicate

literal user input.
variable user input.
`literal system responses.`

The following administrative operations are available in the SSE interface to the BAM server:

- adding a user and password
- reducing user permissions to read-only
- changing the password for a user

To add a user for administrative sessions, enter the following `telnet` command:
`config add user` ***`user password password`***

The second instance of ***`password`*** is a required confirmation.

By default, a new user is given both read and write access. To restrict access to read-only, enter the following `telnet` command:
`config modify level user 1`

To change the password for the specified ***`user`*** in the `telnet` user list, enter the following `telnet` command:
`config change pass user password password`

The first instance of ***`password`*** is the new password. The second instance of ***`password`*** is a required confirmation of the new password.

22.3.3 Overriding Forgotten IP Addresses or Passwords on AP, SM, or BH

Canopy systems offer a plug that allows you to temporarily override some AP/SM/BH settings and thereby regain control of the module. This plug is needed for access to the module in any of the following cases:

- You have forgotten either
  - the IP address assigned to the module.
  - the password that provides access to the module.
- The module has been locked by the No Remote Access feature. (See Denying All Remote Access on Page 360 and Reinstating Remote Access Capability on Page 360.)
- You want local access to a module that has had the 802.3 link disabled in the Configuration page.

This override plug resets the LAN1 IP address to 169.254.1.1. The plug allows you to access the module through the default configuration *without changing* the configuration. You can then view and reset any non-default values.

Acquiring the Override Plug

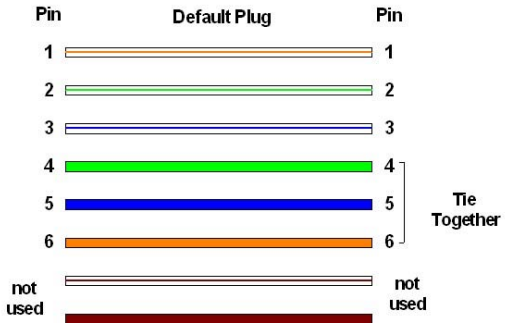
You can either purchase or fabricate an override plug as follows. To purchase an override plug for a nominal fee, order the plug at http://www.best-tronics.com/motorola. To fabricate an override plug, perform the following steps.

Procedure 40: Fabricating an override plug

1. Install an RJ-11 6-pin connector onto a 6-inch length of CAT 5 cable.
2. Pin out all 6-pins.

3. Short (solder together) Pins 4 and 6 on the other end. Do not connect any other wires to anything. The result should be as follows:

Pin 1 → white / orange	← Pin 1
Pin 2 → white / green	← Pin 2
Pin 3 → white / blue	← Pin 3
Pin 4 → green	← Pin 6
Pin 5 → blue	← Pin 5
Pin 6 → orange	← Pin 4



========== **end of procedure** ==========

Using the Override Plug

IMPORTANT!
While the override plug is connected to a module, the module can neither register nor allow registration of another module.

To regain access to the module, perform the following steps.

Procedure 41: Regaining access to a module

1. Insert the override plug into the RJ-11 GPS utility port of the module.
2. Power cycle by removing, then re-inserting, the Ethernet cable.
   RESULT: The module boots with the default IP address of 169.254.1.1, password fields blank, and all other configuration values as previously set.
3. Wait approximately 30 seconds for the boot to complete.
4. Remove the override plug.
5. Set passwords and IP address as desired.
6. Change configuration values if desired.
7. Click **Save Changes**.
8. Click **Reboot**.

========== **end of procedure** ==========

22.3.4 Overriding Forgotten IP Addresses or Passwords on CMMmicro

By using an override toggle switch on the CMMmicro circuit board, you can temporarily override a lost or unknown IP address or password as follows:

- Up is the override position in which a power cycle causes the CMMmicro to boot with the default IP address (169.254.1.1) and no password required.
- Down is the normal position in which a power cycle causes the CMMmicro to boot with your operator-set IP address and password(s).

To override a lost or unknown IP address or password, perform the following steps.

Procedure 42: Using the override switch to regain access to CMMmicro

IMPORTANT!

In override mode

- a CMMmicro provides no power on its ports.
- any APs or BHs connected to the CMMmicro are not powered.
- you cannot gain browser access to the CMMmicro through any connected APs or BHs.

1. Gain physical access to the inside of the CMMmicro enclosure.
2. Establish direct Ethernet connectivity to the CMMmicro (not through an AP or BH).
3. Flip the toggle switch up (toward you).
4. Power cycle the CMMmicro.
   RESULT: The module reboots with the default IP address of 169.254.1.1, password fields blank, and all other configuration values as previously set.
5. Set passwords as desired, or enter a blank space to set no password.
6. Change configuration values if desired.
7. Click **Save Changes**.
8. Flip the toggle switch down (away from you).
9. Click **Reboot**.

========== **end of procedure** ==========

22.4 REQUIRING SM AUTHENTICATION

Through the use of Canopy Bandwidth and Authentication Manager (BAM) software and configurable parameters, you can enhance network security by requiring SMs to authenticate after registering. Beyond the floating license keys for BAM server(s) and APs, three keys and a random number are involved in authentication as follows:

- factory-set key in each SM. Neither the subscriber nor the network operator can view or change this key.
- authentication key, also known as authorization key and skey. The network operator sets this key both in the Configuration page of the SM and in the ESN

database. In the **Authentication Key** parameter of the SM Configuration web page, password access to the page governs whether the network operator or the subscriber can view and set this key.

- random number, generated by BAM and used in each attempt by an SM to register and authenticate. Neither the subscriber nor the network operator can view this number.
- session key, calculated separately by the SM and BAM, based on both the authentication key (or, by default, the factory-set key) and the random number. BAM sends the session key to the AP. Neither the subscriber nor the network operator can view this key.

None of the above keys is ever sent in an over-the-air link during an SM registration attempt. However, with the assumed security risk, the operator can create and configure an authentication key in the **Authentication Key** field of the SM Configuration page. See Authentication Key on Page 212.

22.5 FILTERING PROTOCOLS AND PORTS

In Canopy System Release 4.2 and later releases, you can filter (block) specified protocols and ports from leaving the SM and entering the Canopy network. This protects the network from both intended and inadvertent packet loading or probing by network users. By keeping the specified protocols or ports off the network, this feature also provides a level of protection to users from each other.

Protocol and port filtering is set per SM. Except for filtering of SNMP ports, filtering occurs as packets leave the SM. If an SM is configured to filter SNMP, then SNMP packets are blocked from entering the SM and, thereby, from interacting with the SNMP portion of the protocol stack on the SM.

22.5.1 Port Filtering with NAT Enabled

Where NAT is enabled, you can filter only the three user-defined ports. The following are example situations in which you can configure port filtering where NAT is enabled.

- To block a subscriber from using FTP, you can filter Ports 20 and 21 (the FTP ports) for both the TCP and UDP protocols.
- To block a subscriber from access to SNMP, you can filter Ports 161 and 162 (the SNMP ports) for both the TCP and UDP protocols.
  NOTE: In only the SNMP case, filtering occurs before the packet interacts with the protocol stack.

22.5.2 Protocol and Port Filtering with NAT Disabled

Where NAT is disabled, you can filter both protocols and the three user-defined ports. Using the check boxes on the interface, you can either

- allow all protocols except those that you wish to block.
- block all protocols except those that you wish to allow.

You can allow or block any of the following protocols:

- PPPoE (Point to Point Protocol over Ethernet)
- Any or all of the following IPv4 (Internet Protocol version 4) protocols:
  - SMB (Network Neighborhood)
  - SNMP
  - Up to 3 user-defined ports
  - All other IPv4 traffic (see Figure 117)
- Uplink Broadcast
- ARP (Address Resolution Protocol)
- All others (see Figure 117)

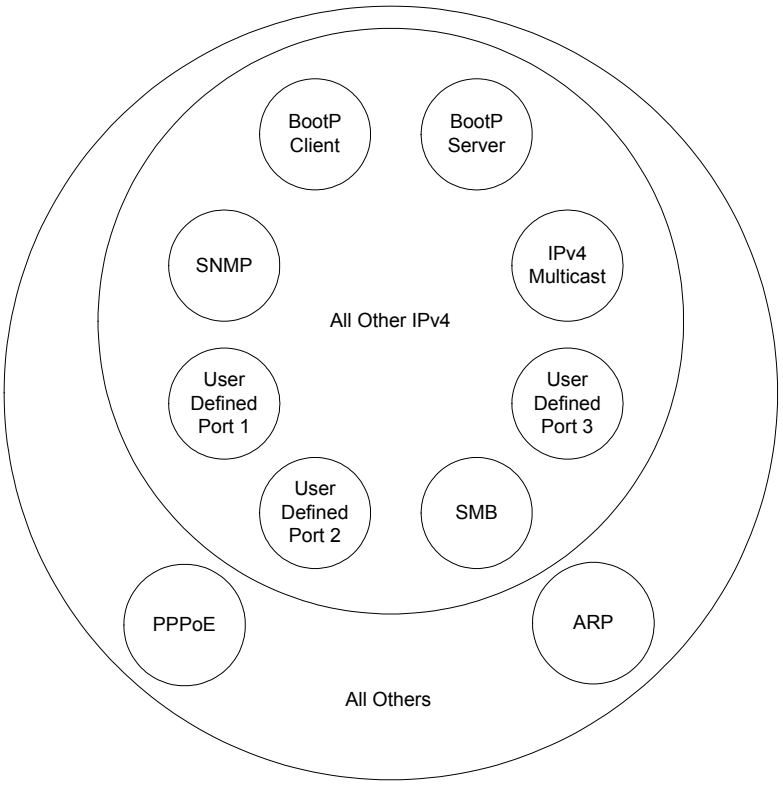


Figure 117: Categorical protocol filtering

The following are example situations in which you can configure protocol filtering where NAT is disabled:

- If you block a subscriber from only PPoE and SNMP, then the subscriber retains access to all other protocols and all ports.
- If you block PPoE, IPv4, and Uplink Broadcast, and you also check the **All others** selection, then only Address Resolution Protocol is not filtered.

The ports that are filtered as a result of protocol selections in the Packet Filter Configuration block of the Advanced Network Configuration page in the SM are listed in Table 52.

Table 52: Ports filtered per protocol selections

Protocol Selected	Port Filtered (Blocked)
SMB	Destination Ports 137 TCP and UDP, 138 UDP, 139 TCP, 445 TCP
SNMP	Destination Ports 161 TCP and UDP, 162 TCP and UDP
Bootp Client	Source Port 68 UDP
Bootp Server	Source Port 67 UDP

22.6 ENCRYPTING DOWNLINK BROADCASTS

In Canopy System Release 4.2 and later releases, an AP can be enabled to encrypt downlink broadcast packets such as the following:

- ARP
- NetBIOS
- broadcast packets containing video data on UDP.

However, before the Encrypt Downlink Broadcast feature is enabled on the AP

- air link security should be enabled on the AP.
- all SMs that register to the AP *must* operate on Release 4.2 or later release.

CAUTION!
An SM that operates on an earlier release cannot decrypt encrypted broadcasts and, consequently, drops connectivity (or cannot establish a link with) with the AP that is configured to encrypt downlink broadcasts.

The encryption used is DES for a DES module, and AES for an AES module.

23 MANAGING BANDWIDTH AND AUTHENTICATION

This section provides a high-level description of BAM in a Canopy network. For more specific information, see *Canopy Bandwidth and Authentication Manager (BAM) User Guide*.

23.1 MANAGING BANDWIDTH WITHOUT BAM

Unless BAM is deployed and is configured in the AP, bandwidth management is limited to applying a single sustained data rate value (for uplink and for downlink) and a single burst allocation value (for uplink and for downlink) to every SM that registers in the AP.

23.2 BANDWIDTH AND AUTHENTICATION MANAGER (BAM) SERVICES AND FEATURES

BAM enables you to perform the following management operations on SMs:

- Change the key that the SM(s) need for authenticating.
- Temporarily suspend or reinstate a subscriber.
- Set burst size and data transfer rate caps for an SM or group of SMs.
- Use licensing to uncap an SM or group of SMs.
- List all ESNs that are associated with a specified VLAN ID.
- Associate or dissociate an SM or group of SMs with a specified VLAN ID.
- Set VLAN parameters.
- Toggle whether to send those VLAN parameters to the SM(s).
- Set CIR parameters for low-priority and high-priority channel rates.
- Toggle whether to send those CIR parameters to the SM(s).
- Toggle whether to enable the high-priority channel in the SM(s).

23.2.1 Bandwidth Manager Capability

Canopy Bandwidth and Authentication Manager (BAM) software allows you to set per-SM bandwidth for a sustained rate and for a burst rate. With this capability, the Canopy system allows both

- burst rates beyond those of many other broadband access solutions.
- control of average bandwidth allocation to prevent excessive bandwidth usage by a subscriber.

All packet throttling occurs in the SMs and APs based on Quality of Service (QoS) data that the BAM server provides. No BAM server processing power or network messages are needed for packet throttling.

QoS management also supports marketing of broadband connections at various data rates, for operator-defined groups of subscribers, and at various price points. This allows you to meet customer needs at a price that the customer deems reasonable and affordable.

When BAM *is* enabled in the AP Configuration page, bandwidth management is expanded to apply uniquely specified sustained data rate and burst allocation values to each registered SM. Thus, you can define differently priced tiers of subscriber service.

Designing Tiered Subscriber Service Levels

Examples of levels of service that vary by bandwidth capability are provided in Table 53.

NOTE:
The services that Table 53 correlate to service levels are best cases. These do not account for

- transient limitations such as congestion on the Internet.
- network configuration limitations such as server-side bandwidth capability.

Table 53: Examples of SM tiers

Rate	Basic Service	Enhanced Service	Premium Service
Sustained Uplink and Sustained Downlink Rates	128 kbps	512 kbps	No restrictions
Uplink Burst and Downlink Burst Sizes	40,000 kb (5 MB)	80,000 kb (10 MB)	No restrictions
Initial burst speed	2.5 Mbps	2.5 Mbps	2.5 Mbps
Time to download medium complexity web page	1 sec	1 sec	1 sec
Time to download 5 MB	16 sec	16 sec	16 sec
Time to download 10 MB	336 sec	32 sec	32 sec
Time to download 25 MB	1296 sec (over 20 min)	272 sec	80 sec

23.2.2 Authentication Manager Capability

BAM software allows you to set per AP a requirement that each SM registering to the AP must authenticate. When AP Authentication Server (APAS) is enabled in the AP, any SM that attempts to register to the AP is denied service if authentication fails, such as (but not limited to) when no BAM server is operating or when the SM is not listed in the database.

If a BAM server drops out of service where no redundant BAM server exists

- an SM that attempts to register is denied service.
- an SM that is already in session remains in session

In a typical Canopy network, some SMs re-register daily (when subscribers power down the SMs, for example), and others do not re-register in a period of several weeks. Whenever an authentication attempt fails, the SM locks out of any other attempt to register itself to the same AP for the next 15 minutes.

24 MANAGING THROUGH A NETWORK MANAGEMENT STATION (NMS)

SNMPv2 (Simple Network Management Protocol Version 2) can be used to manage and monitor the Canopy modules under SMI (Structure of Management Information) specifications. SMI specifies management information definitions in ASN.1 (Abstract Syntax Notation One) language. SNMPv2 supports both 32-bit and 64-bit counters. The SMI for SNMPv2 is defined in RFC 1902 at http://www.faqs.org/rfcs/rfc1902.html.

24.1 ROLES OF HARDWARE AND SOFTWARE ELEMENTS

24.1.1 Role of the Agent

In SNMP, software on each managed device acts as the *agent*. The agent collects and stores management information in ASN.1 format, in a structure that a MIB (management information base) defines. The agent responds to commands to

- send information about the managed device.
- modify specific data on the managed device.

24.1.2 Role of the Managed Device

In SNMP, the managed device is the network element that operates on the agent software. In the Canopy network, this managed device is the module (AP, SM, or BH). With the agent software, the managed device has the role of server in the context of network management.

24.1.3 Role of the NMS

In SNMP, the NMS (network management station) has the role of client. An application (manager software) operates on the NMS to manage and monitor the modules in the network through interface with the agents.

24.1.4 Dual Roles for the NMS

The NMS can simultaneously act as an agent. In such an implementation, the NMS acts as

- client to the agents in the modules, when polling for the agents for information and sending modification data to the agents.
- server to another NMS. when being polled for information gathered from the agents and receiving modification data to send to the agents.

24.1.5 Simple Network Management Protocol (SNMP) Commands

To manage a module, SNMPv2 supports the `set` command, which instructs the agent to change the data that manages the module.

To monitor a network element (Canopy module), SNMPv2 supports

- the `get` command, which instructs the agent to send information about the module to the manager in the NMS.
- traversal operations, which the manager uses to identify supported objects and to format information about those objects into relational tables.

In a typical Canopy network, the manager issues these commands to the agents of more than one module (to all SMs in the operator network, for example).

24.1.6 Traps from the Agent

When a specified event occurs in the module, the agent initiates a trap, for which the agent sends an unsolicited asynchronous message to the manager.

24.2 MANAGEMENT INFORMATION BASE (MIB)

The MIB, the SNMP-defined data structure, is a tree of standard branches that lead to optional,
non-standard positions in the data hierarchy. The MIB contains both

- objects that SNMP is allowed to control (bandwidth allocation or access, for example)
- objects that SNMP is allowed to monitor (packet transfer, bit rate, and error data, for example).

The path to each object in the MIB is unique to the object. The endpoint of the path is the object identifier.

24.2.1 Cascading Path to the MIB

The standard MIB hierarchy includes the following cascading branch structures:

- the top (standard body) level:
  - ccitt (0)
  - **iso (1)**
  - iso-ccitt (2)
- under iso (1) above:
  - standard (0)
  - registration-authority (1)
  - member-body (2)
  - **identified-organization (3)**
- under identified-organization (3) above:
  - dod (6)
  - other branches
- under dod (6) above:
  - internet (1)
  - other branches

- under internet (1) above:
  - mgmt (2)
  - private (4)
  - other branches
- under mgmt (2) above: **mib-2 (1)** and other branches. (See MIB-II below.)

  under private (4) above: **enterprise (1)** and other branches. (See Canopy Enterprise MIB below.)

  Beneath this level are non-standard branches that the enterprise may define.

Thus, the path to an object that is managed under MIB-II begins with the decimal string **1.3.6.1.2.1** and ends with the object identifier and instance(s), and the path to an object that is managed under the Canopy Enterprise MIB begins with **1.3.6.1.4.1**, and ends with the object identifier and instance(s).

24.2.2 Object Instances

An object in the MIB can have either only a single instance or multiple instances, as follows:

- a scalar object has only a single instance. A reference to this instance is designated by `.0`, following the object identifier.
- a tabular object has multiple instances that are related to each other. Tables in the MIB associate these instances. References to these instances typically are designated by `.1`, `.2`, and so forth, following the object identifier.

24.2.3 Management Information Base Systems and Interface (MIB-II)

The standard MIB-II (Management Information Base systems and interface) objects are programmed into the Canopy modules. To read this MIB, see *Management Information Base for Network Management of TCP/IP-based Internets: MIB II*, RFC 1213 at http://www.faqs.org/rfcs/rfc1213.html.

The MIB-II standard categorizes each object as one of the types defined in Table 54.

Table 54: Categories of MIB-II objects

Objects in category…	Control or identify the status of…
system	system operations in the module.
interfaces	the network interfaces for which the module is configured.
ip	Internet Protocol information in the module.
icmp	Internet Control Message Protocol information in the module. (These messages flag IP problems and allow IP links to be tested.)
tcp	Transport Control Protocol information in the module (to control and ensure the flow of data on the Internet).
udp	User Datagram Protocol information in the module (for checksum and address).

24.2.4 Canopy Enterprise MIB

For additional reporting and control, the Canopy Releases 3.2.5 and later provide the Canopy Enterprise MIB, which extends the objects for any NMS that uses SNMP interaction. This MIB comprises five text files that are formatted in standard ASN.1 (Abstract Syntax Notation One) language.

To use this MIB, perform the following steps.

Procedure 43: Installing the Canopy Enterprise MIB files

1. On the NMS, immediately beneath the `root` directory, create directory *`mibviewer`*.
2. Immediately beneath the *`mibviewer`* directory, create directory *`canopymibs`*.
3. Download the following three standard MIB files from http://www.simpleweb.org/ietf/mibs into the *`mibviewer/canopymibs`* directory on the NMS:
   - SNMPv2-SMI.txt, which defines the Structure of Management Information specifications.
   - SNMPv2-CONF.txt, which allows macros to be defined for object group, notification group, module compliance, and agent capabilities.
   - SNMPv2-TC.txt, which defines general textual conventions.
4. Move the following five files from your Canopy software package directory into the *`mibviewer/canopymibs`* directory on the NMS (if necessary, first download the software package from http://www.motorola.com/canopy):
   - `whisp-tcv2-mib.txt` (Textual Conventions MIB), which defines Canopy system-specific textual conventions
   - `WHISP-GLOBAL-REG-MIB.txt` (Registrations MIB), which defines registrations for global items such as product identities and product components.
   - `WHISP-BOX-MIBV2-MIB.txt` (Box MIB), which defines module-level (AP, SM, and BH) objects.
   - `WHISP-APS-MIB.txt` (APs MIB), which defines objects that are specific to the AP or BH timing master.
   - `WHISP-SM-MIB.txt` (SM MIB), which defines objects that are specific to the SM or BH timing slave.
   - `CMM3-MIB.txt` (CMM3 MIB), which defines objects that are specific to the CMMmicro.

IMPORTANT!
Do not edit these MIB files in ASN.1. These files are intended for manipulation by only the NMS. However, you can view these files through a commercially available MIB viewer. Such viewers are listed under Traps Provided in the Canopy 45-Mbps BH Module MIB on Page 326.

5. Download a selected MIB viewer into directory `mibviewer`.
6. As instructed by the user documentation that supports your NMS, import the eight MIB files that are listed above.

24.3 CONFIGURING MODULES FOR SNMP ACCESS

Canopy modules provide the following Configuration web page parameters that govern SNMP access from the manager to the agent:

- **Display-Only Access**, which specifies the password that allows only viewing.
- **Full Access**, which specifies the password that allows both viewing and changing.
- **Community String**, which specifies the password for security between managers and the agent.
- **Accessing Subnet**, which specifies the subnet mask allows managers to poll the agents.
- **Trap Address**, which specifies the IP address of the NMS.

For more information about each of these fields, see the user document that supports the module.

24.4 OBJECTS DEFINED IN THE CANOPY ENTERPRISE MIB

The Canopy Enterprise MIB defines objects for

- APs and BH timing masters
- SMs and BH timing slaves
- CMMmicros

NOTE:
The 45-Mbps BH does not support these objects. The MIBs that this module supports are listed under Objects Defined in the Canopy 45-Mbps BH Module MIB on Page 324.

24.4.1 AP, SM, and BH Objects

The objects that the Canopy Enterprise MIB defines for each AP and BH Timing Master are listed in Table 55.

Table 55: Canopy Enterprise MIB objects for APs, SMs, and BHs

AP, SM, BH Object Name	Value Syntax	Operation Allowed
addVlanMember	Integer	manage and/or monitor
agingTimeout	Integer	manage and/or monitor
antennaGain	Integer	manage and/or monitor
bhModulation	Integer	manage and/or monitor
bhTimingMode	Integer	manage and/or monitor
bridgeEntryTimeout	Integer	manage and/or monitor
clearEventLog	Integer	manage and/or monitor
colorCode	Integer	manage and/or monitor
displayOnlyAccess	DisplayString	manage and/or monitor
dynamicLearning	Integer	manage and/or monitor
eirp	Integer	manage and/or monitor
extFilterDelay	Integer	manage and/or monitor
fullAccess	DisplayString	manage and/or monitor
linkNegoSpeed	DisplayString	manage and/or monitor
managementVID	Integer	manage and/or monitor
powerControl	Integer	manage and/or monitor
reboot	Integer	manage and/or monitor
removeVlanMember	Integer	manage and/or monitor
scheduling	Integer	manage and/or monitor
snmpMibPerm	Integer	manage and/or monitor
taggedFrame	Integer	manage and/or monitor
transmitterOP	Integer	manage and/or monitor
webAutoUpdate	Integer	manage and/or monitor
boxDeviceType	DisplayString	monitor
boxDeviceTypeID	DisplayString	monitor
boxEncryption	DisplayString	monitor
boxFrequency	DisplayString	monitor
etherLinkStatus	DisplayString	monitor
boxTemperature	DisplayString	monitor
pass1Status	DisplayString	monitor
pass2Status	DisplayString	monitor
platformVer	Integer	monitor

AP, SM, BH Object Name	Value Syntax	Operation Allowed
whispBoxBoot	DisplayString	monitor
whispBoxEsn	WhispMACAddress	monitor
whispBoxEvntLog	EventString	monitor
whispBoxFPGAVer	DisplayString	monitor
whispBoxSoftwareVer	DisplayString	monitor
whispBridgeAge	Integer	monitor
whispBridgeDesLuid	WhispLUID	monitor
whispBridgeExt	Integer	monitor
whispBridgeHash	Integer	monitor
whispBridgeMacAddr	MacAddress	monitor
whispBridgeTbErr	Integer	monitor
whispBridgeTbFree	Integer	monitor
whispBridgeTbUsed	Integer	monitor
whispVAge	Integer	monitor
whispVID	Integer	monitor
whispVType	DisplayString	monitor

24.4.2 AP and BH Timing Master Objects

The objects that the Canopy Enterprise MIB defines for each AP and BH Timing Master are listed in Table 56. The highlighted objects are commonly monitored by the manager. The traps provided in this set of objects are listed under Traps Provided in the Canopy Enterprise MIB on Page 325.

Table 56: Canopy Enterprise MIB objects for APs and BH timing masters

AP, BHM Object Name	Value Syntax	Operation Allowed
apBeaconInfo	Integer	manage and/or monitor
asIP1	IpAddress	manage and/or monitor
asIP2	IpAddress	manage and/or monitor
asIP3	IpAddress	manage and/or monitor
authKey	DisplayString	manage and/or monitor
authMode	Integer	manage and/or monitor
berMode	Integer	manage and/or monitor
broadcastRetryCount	Integer	manage and/or monitor
configSource	Integer	manage and/or monitor

AP, BHM Object Name	Value Syntax	Operation Allowed
dAcksReservHigh	Integer	manage and/or monitor
defaultGw	IpAddress	manage and/or monitor
dfsConfig	Integer	manage and/or monitor
dwnLnkData	Integer	manage and/or monitor
dwnLnkDataRate	Integer	manage and/or monitor
dwnLnkLimit	Integer	manage and/or monitor
encryptDwBroadcast	Integer	manage and/or monitor
encryptionMode	Integer	manage and/or monitor
gpsInput	Integer	manage and/or monitor
gpsTrap	Integer	manage and/or monitor
highPriorityUpLnkPct	Integer	manage and/or monitor
lanIp	IpAddress	manage and/or monitor
lanMask	IpAddress	manage and/or monitor
linkTestAction	Integer	manage and/or monitor
linkTestDuration	Integer	manage and/or monitor
linkTestLUID	Integer	manage and/or monitor
maxRange	Integer	manage and/or monitor
ntpServerIP	IpAddress	manage and/or monitor
numCtlSlots	Integer	manage and/or monitor
numCtlSlotsReserveHigh	Integer	manage and/or monitor
numDAckSlots	Integer	manage and/or monitor
numUAckSlots	Integer	manage and/or monitor
privateIp	IpAddress	manage and/or monitor
regTrap	Integer	manage and/or monitor
rfFreqCarrier	Integer	manage and/or monitor
sectorID	Integer	manage and/or monitor
txSpreading	Integer	manage and/or monitor
uAcksReservHigh	Integer	manage and/or monitor
updateAppAddress	IpAddress	manage and/or monitor
upLnkDataRate	Integer	manage and/or monitor
upLnkLimit	Integer	manage and/or monitor
vlanEnable	Integer	manage and/or monitor
actDwnFragCount	Gauge32	monitor

AP, BHM Object Name	Value Syntax	Operation Allowed
actDwnLinkIndex	Integer	monitor
actUpFragCount	Gauge32	monitor
adaptRate	DisplayString	monitor
avgPowerLevel	DisplayString	monitor
dataSlotDwn	Integer	monitor
dataSlotUp	Integer	monitor
dataSlotUpHi	Integer	monitor
dfsStatus	DisplayString	monitor
downLinkEff	Integer	monitor
downLinkRate	Integer	monitor
dwnLnkAckSlot	Integer	monitor
dwnLnkAckSlotHi	Integer	monitor
expDwnFragCount	Gauge32	monitor
expUpFragCount	Gauge32	monitor
fpgaVersion	DisplayString	monitor
gpsStatus	DisplayString	monitor
lastPowerLevel	DisplayString	monitor
linkAirDelay	Integer	monitor
linkAveJitter	Integer	monitor
linkDescr	DisplayString	monitor
linkESN	PhysAddress	monitor
linkInDiscards	Counter32	monitor
linkInError	Counter32	monitor
linkInNUcastPkts	Counter32	monitor
linkInOctets	Counter32	monitor
linkInUcastPkts	Counter32	monitor
linkInUnknownProtos	Counter32	monitor
linkLastJitter	Integer	monitor
linkLastRSSI	Integer	monitor
linkLUID	Integer	monitor
linkMtu	Integer	monitor
linkOutDiscards	Counter32	monitor
linkOutError	Counter32	monitor

AP, BHM Object Name	Value Syntax	Operation Allowed
linkOutNUcastPkts	Counter32	monitor
linkOutOctets	Counter32	monitor
linkOutQLen	Gauge32	monitor
linkOutUcastPkts	Counter32	monitor
linkRegCount	Integer	monitor
linkReRegCount	Integer	monitor
linkRSSI	Integer	monitor
linkSessState	Integer	monitor
linkSiteName	DisplayString	monitor
linkSpeed	Gauge32	monitor
linkTestError	DisplayString	monitor
linkTestStatus	DisplayString	monitor
linkTimeOut	Integer	monitor
maxDwnLinkIndex	Integer	monitor
numCtrSlot	Integer	monitor
numCtrSlotHi	Integer	monitor
PhysAddress	PhysAddress	monitor
radioSlicing	Integer	monitor
radioTxGain	Integer	monitor
regCount	Integer	monitor
sesDownlinkLimit	Integer	monitor
sesDownlinkRate	Integer	monitor
sesUplinkLimit	Integer	monitor
sesUplinkRate	Integer	monitor
sessionCount	Integer	monitor
softwareBootVersion	DisplayString	monitor
softwareVersion	DisplayString	monitor
testDuration	Integer	monitor
testLUID	Integer	monitor
upLinkEff	Integer	monitor
upLinkRate	Integer	monitor
upLnkAckSlot	Integer	monitor

AP, BHM Object Name	Value Syntax	Operation Allowed
upLnkAckSlotHi	Integer	monitor
whispGPSStats	Integer	monitor

24.4.3 SM and BH Timing Slave Objects

The objects that the Canopy Enterprise MIB defines for each SM and BH Timing Slave are listed in Table 57. The highlighted objects are commonly monitored by the manager.

Table 57: Canopy Enterprise MIB objects for SMs and BH timing slaves

SM, BHS Object Name	Value Syntax	Operation Allowed
allOtherIPFilter	Integer	manage and/or monitor
allOthersFilter	Integer	manage and/or monitor
alternateDNSIP	IpAddress	manage and/or monitor
arpCacheTimeout	Integer	manage and/or monitor
arpFilter	Integer	manage and/or monitor
authKey	DisplayString	manage and/or monitor
authKeyOption	Integer	manage and/or monitor
bootpcFilter	Integer	manage and/or monitor
bootpsFilter	Integer	manage and/or monitor
defaultGw	IpAddress	manage and/or monitor
dhcpClientEnable	Integer	manage and/or monitor
dhcpIPStart	IpAddress	manage and/or monitor
dhcpNumIPsToLease	Integer	manage and/or monitor
dhcpServerEnable	Integer	manage and/or monitor
dhcpServerLeaseTime	Integer	manage and/or monitor
dmzEnable	Integer	manage and/or monitor
dmzIP	IpAddress	manage and/or monitor
dnsAutomatic	Integer	manage and/or monitor
enable8023link	Integer	manage and/or monitor
hiPriorityChannel	Integer	manage and/or monitor
hiPriorityDownlinkCIR	Integer	manage and/or monitor
hiPriorityUplinkCIR	Integer	manage and/or monitor
ingressVID	Integer	manage and/or monitor

SM, BHS Object Name	Value Syntax	Operation Allowed
ip4MultFilter	Integer	manage and/or monitor
lanIp	IpAddress	manage and/or monitor
lanMask	IpAddress	manage and/or monitor
lowPriorityDownlinkCIR	Integer	manage and/or monitor
lowPriorityUplinkCIR	Integer	manage and/or monitor
naptEnable	Integer	manage and/or monitor
naptPrivateIP	IpAddress	manage and/or monitor
naptPrivateSubnetMask	IpAddress	manage and/or monitor
naptPublicGatewayIP	IpAddress	manage and/or monitor
naptPublicIP	IpAddress	manage and/or monitor
naptPublicSubnetMask	IpAddress	manage and/or monitor
naptRFPublicGateway	IpAddress	manage and/or monitor
naptRFPublicIP	IpAddress	manage and/or monitor
naptRFPublicSubnetMask	IpAddress	manage and/or monitor
networkAccess	Integer	manage and/or monitor
port1TCPFilter	Integer	manage and/or monitor
port2TCPFilter	Integer	manage and/or monitor
port3TCPFilter	Integer	manage and/or monitor
port1UDPFilter	Integer	manage and/or monitor
port2UDPFilter	Integer	manage and/or monitor
port3UDPFilter	Integer	manage and/or monitor
powerUpMode	Integer	manage and/or monitor
pppoeFilter	Integer	manage and/or monitor
prefferedDNSIP	IpAddress	manage and/or monitor
rfScanList	DisplayString	manage and/or monitor
smbFilter	Integer	manage and/or monitor
snmpFilter	Integer	manage and/or monitor
tcpGarbageCollectTmout	Integer	manage and/or monitor
timingPulseGated	Integer	manage and/or monitor
twoXRate	Integer	manage and/or monitor
udpGarbageCollectTmout	Integer	manage and/or monitor
uplinkBCastFilter	Integer	manage and/or monitor
userDefinedPort1	Integer	manage and/or monitor

SM, BHS Object Name	Value Syntax	Operation Allowed
userDefinedPort2	Integer	manage and/or monitor
userDefinedPort3	Integer	manage and/or monitor
userP1Filter	Integer	manage and/or monitor
userP2Filter	Integer	manage and/or monitor
userP3Filter	Integer	manage and/or monitor
adaptRate	DisplayString	monitor
airDelay	Integer	monitor
calibrationStatus	DisplayString	monitor
dhcpcdns1	IpAddress	monitor
dhcpcdns2	IpAddress	monitor
dhcpcdns3	IpAddress	monitor
dhcpCip	IpAddress	monitor
dhcpClientLease	TimeTicks	monitor
dhcpCSMask	IpAddress	monitor
dhcpDfltRterIP	IpAddress	monitor
dhcpDomName	DisplayString	monitor
dhcpServerTable	DhcpServerEntry	monitor
dhcpSip	IpAddress	monitor
hostIp	IpAddress	monitor
hostLease	TimeTicks	monitor
hostMacAddress	PhysAddress	monitor
jitter	Integer	monitor
radioDbm	DisplayString	monitor
radioSlicing	Integer	monitor
radioTxGain	Integer	monitor
registeredToAp	DisplayString	monitor
rssi	Integer	monitor
sessionStatus	DisplayString	monitor

24.4.4 CMMmicro Objects

The objects that the Canopy Enterprise MIB defines for each CMMmicro are listed in Table 58.

Table 58: Canopy Enterprise MIB objects for CMMmicros

CMMmicro Object Name	Value Syntax	Operation Allowed
clearEventLog	Integer	manage and/or monitor
defaultGateWay	IpAddress	manage and/or monitor
displayOnlyAccess	DisplayString	manage and/or monitor
fullAccess	DisplayString	manage and/or monitor
gpsTimingPulse	Integer	manage and/or monitor
lan1Ip	IpAddress	manage and/or monitor
lan1SubnetMask	IpAddress	manage and/or monitor
port1Config	Integer	manage and/or monitor
port1Description	DisplayString	manage and/or monitor
port1PowerCtr	Integer	manage and/or monitor
port2Config	Integer	manage and/or monitor
port2Description	DisplayString	manage and/or monitor
port2PowerCtr	Integer	manage and/or monitor
port3Config	Integer	manage and/or monitor
port3Description	DisplayString	manage and/or monitor
port3PowerCtr	Integer	manage and/or monitor
port4Config	Integer	manage and/or monitor
port4Description	DisplayString	manage and/or monitor
port4PowerCtr	Integer	manage and/or monitor
port5Config	Integer	manage and/or monitor
port5Description	DisplayString	manage and/or monitor
port5PowerCtr	Integer	manage and/or monitor
port6Config	Integer	manage and/or monitor
port6Description	DisplayString	manage and/or monitor
port6PowerCtr	Integer	manage and/or monitor
port7Config	Integer	manage and/or monitor
port7Description	DisplayString	manage and/or monitor
port7PowerCtr	Integer	manage and/or monitor
port8Config	Integer	manage and/or monitor

CMMmicro Object Name	Value Syntax	Operation Allowed
port8Description	DisplayString	manage and/or monitor
port8PowerCtr	Integer	manage and/or monitor
reboot	Integer	manage and/or monitor
webAutoUpdate	Integer	manage and/or monitor
deviceType	DisplayString	monitor
displayOnlyStatus	DisplayString	monitor
duplexStatus	Integer	monitor
eventLog	EventString	monitor
fullAccessStatus	DisplayString	monitor
gpsAntennaConnection	DisplayString	monitor
gpsDate	DisplayString	monitor
gpsHeight	DisplayString	monitor
gpsInvalidMsg	DisplayString	monitor
gpsLatitude	DisplayString	monitor
gpsLongitude	DisplayString	monitor
gpsReceiverInfo	DisplayString	monitor
gpsRestartCount	Integer	monitor
gpsSatellitesTracked	DisplayString	monitor
gpsSatellitesVisible	DisplayString	monitor
gpsTime	DisplayString	monitor
gpsTrackingMode	DisplayString	monitor
height	DisplayString	monitor
latitude	DisplayString	monitor
linkSpeed	Integer	monitor
linkStatus	Integer	monitor
longitude	DisplayString	monitor
macAddress	DisplayString	monitor
pkts1024to1522Octets	Counter32	monitor
pkts128to255Octets	Counter32	monitor
pkts256to511Octets	Counter32	monitor
pkts512to1023Octets	Counter32	monitor
pkts64Octets	Counter32	monitor
pkts65to127Octets	Counter32	monitor

CMMmicro Object Name	Value Syntax	Operation Allowed
pldVersion	DisplayString	monitor
portIndex	Integer	monitor
portNumber	Integer	monitor
powerStatus	Integer	monitor
rxAlignmentErrors	Counter32	monitor
rxBroadcastPkts	Counter32	monitor
rxDropPkts	Counter32	monitor
rxExcessSizeDisc	Counter32	monitor
rxFCSErrors	Counter32	monitor
rxFragments	Counter32	monitor
rxGoodOctets	Counter64	monitor
rxJabbers	Counter32	monitor
rxMulticastPkts	Counter32	monitor
rxOctets	Counter64	monitor
rxOversizePkts	Counter32	monitor
rxPausePkts	Counter32	monitor
rxSAChanges	Counter32	monitor
rxSymbolErrors	Counter32	monitor
rxUndersizePkts	Counter32	monitor
rxUnicastPkts	Counter32	monitor
satellitesTracked	DisplayString	monitor
satellitesVisible	DisplayString	monitor
softwareVersion	DisplayString	monitor
syncStatus	DisplayString	monitor
systemTime	DisplayString	monitor
trackingMode	DisplayString	monitor
txBroadcastPkts	Counter32	monitor
txCollisions	Counter32	monitor
txDeferredTransmit	Counter32	monitor
txDropPkts	Counter32	monitor
txExcessiveCollision	Counter32	monitor
txFrameInDisc	Counter32	monitor
txLateCollision	Counter32	monitor

CMMmicro Object Name	Value Syntax	Operation Allowed
txMulticastPkts	Counter32	monitor
txMultipleCollision	Counter32	monitor
txOctets	Counter64	monitor
txPausePkts	Counter32	monitor
txSingleCollision	Counter32	monitor
txUnicastPkts	Counter32	monitor
upTime	DisplayString	monitor

24.5 OBJECTS DEFINED IN THE CANOPY 45-Mbps BH MODULE MIB

The objects that the Canopy 45-Mbps BH module MIB defines are listed in Table 60.

Table 59: Canopy 45-Mbps BH module MIB objects

AP, SM, BH Object Name	Value Syntax	Operation Allowed
iPAddress	IpAddress	manage and/or monitor
subnetMask	IpAddress	manage and/or monitor
gatewayIPAddress	IpAddress	manage and/or monitor
targetMACAddress[1]	DisplayString	manage and/or monitor
masterSlaveMode	Integer	manage and/or monitor
maximumTransmitPower	Integer	manage and/or monitor
receivePower[2]	Integer	manage and/or monitor
vectorError[2]	Integer	manage and/or monitor
transmitPower[2]	Integer	manage and/or monitor
range	Integer	manage and/or monitor
linkLoss[2]	Integer	manage and/or monitor
receiveChannel	Integer	manage and/or monitor
transmitChannel	Integer	manage and/or monitor
receiveModulationMode	Integer	manage and/or monitor
transmitModulationMode	Integer	manage and/or monitor
receiveSnr[2]	Integer	manage and/or monitor
systemReset	Integer	monitor

AP, SM, BH Object Name	Value Syntax	Operation Allowed
softwareVersion	DisplayString	monitor
hardwareVersion	DisplayString	monitor
NOTES: 1. Of the other BH in the link. 2. *max*, *mean*, *min*, *last* during the past hour.		

24.6 INTERFACE DESIGNATIONS IN SNMP

SNMP identifies the ports of the module as follows:

- Interface 1 represents the RF interface of the module. To monitor the status of Interface 1 is to monitor the traffic on the RF interface.
- Interface 2 represents the Ethernet interface of the module. To monitor the status of Interface 2 is to monitor the traffic on the Ethernet interface.

These interfaces can be viewed on the NMS through definitions that are provided in the standard MIB files.

24.7 TRAPS PROVIDED IN THE CANOPY ENTERPRISE MIB

Canopy modules provide the following SNMP traps for automatic notifications to the NMS:

- whispGPSInSync, which signals a transition from not synchronized to synchronized.
- whispGPSOutSync, which signals a transition from synchronized to not synchronized.
- whispRegComplete, which signals registration completed.
- whispRegLost, which signals registration lost.
- whispRedarDetected, which signals that the one-minute scan has been completed, radar has been detected, and the radio will shutdown.
- whispRedarEnd, which signals that the one-minute scan has been completed, radar *has not* been detected, and the radio will resume normal operation.

NOTE:
The 45-Mbps BH does not support the traps listed above.

24.8 TRAPS PROVIDED IN THE CANOPY 45-Mbps BH MODULE MIB

Canopy 45-Mbps BH modules provide the following SNMP traps for automatic notifications to the NMS:

- dfsChannelChangeTrap, which signals that the channel has changed.
- dfsImpulsiveInterferenceDetectedTrap, which signals that impulsive interference has been detected.

24.9 MIB VIEWERS

Any of several commercially available MIB viewers can facilitate management of these objects through SNMP. Some are available as open source software. The Canopy division does not endorse, support, or discourage the use of any these viewers.

To assist end users in this area, the Canopy division offers a starter guide for one of these viewers—MRTG (Multi Router Traffic Grapher). This starter guide is titled ***Canopy*** *Network Management with MRTG: Application Note*, and is available in the Library section under Support at http://www.motorola.com/canopy. MRTG software is available at http://mrtg.hdl.com/mrtg.html.

Other MIB viewers are available and/or described at the following web sites:

http://ns3.ndgsoftware.com/Products/NetBoy30/mibbrowser.html

http://www.adventnet.com/products/snmputilities/

http://www.dart.com/samples/mib.asp

http://www.edge-technologies.com/webFiles/products/nvision/index.cfm

http://www.ipswitch.com/products/whatsup/monitoring.html

http://www.koshna.com/products/KMB/index.asp

http://www.mg-soft.si/mgMibBrowserPE.html

http://www.mibexplorer.com

http://www.netmechanica.com/mibbrowser.html

http://www.networkview.com

http://www.newfreeware.com/search.php3?q=MIB+browser

http://www.nudesignteam.com/walker.html

http://www.oidview.com/oidview.html

http://www.solarwinds.net/Tools

http://www.stargus.com/solutions/xray.html

http://www.totilities.com/Products/MibSurfer/MibSurfer.htm

25 MANAGING THROUGH THE CANOPY NETWORK UPDATER TOOL (CNUT)

The Canopy Network Updater Tool manages and automates the software and firmware upgrade process for Canopy radio and CMMmicro modules across the network. This eliminates the need for an administrator to visit each radio in the network (or each AP while using the Autoupdate feature) to upgrade the modules.

25.1 CNUT FUNCTIONS

The Canopy Network Updater Tool

- automatically discovers all Canopy network elements
- executes a UDP command that initiates and terminates the Autoupdate mode within APs. This command is both secure and convenient:
  - For security, the AP accepts this command from only the IP address that you specify in the Configuration page of the AP.
  - For convenience, Network Updater automatically sets this Configuration parameter in the APs to the IP address of the Network Updater server when the server performs any of the update commands.
- allows you to choose among updating
  - your entire network.
  - only elements that you select.
  - only network branches that you select.
- provides a Script Engine that you can use with any script that
  - you define.
  - Canopy supplies.

25.2 NETWORK ELEMENT GROUPS

With the Canopy Network Updater Tool, you can identify element groups composed of network elements that you select. Identifying these element groups

- organizes the display of elements (for example, by region or by AP cluster).
- allows you to
  - perform an operation on all elements in the group simultaneously.
  - set group-level defaults for telnet or ftp password access and SNMP Community String (defaults that can be overridden in an individual element when necessary).

25.3 NETWORK LAYERS

A typical Canopy network contains multiple layers of elements, each layer lying farther from the Point of Presence. For example, SMs are behind an AP and thus, in this context, at a lower layer than the AP. Correctly portraying these layers in Network Updater is essential so that Network Updater can perform radio and AP cluster upgrades in an appropriate order.

IMPORTANT!
Correct layer information ensures that Network Updater does not command an AP that is behind another AP/SM pair (such as in a remote AP installation) to perform an upgrade at the same time as the SM that is feeding the AP. If this occurs, then the remote AP loses network connection during the upgrade (when the SM in front of the AP completes its upgrade and reboots).

25.4 SCRIPT ENGINE

Script Engine is the capability in Network Updater that executes any user-defined script against any network element or element group. This capability is useful for network management, especially for scripts that you repetitively execute across your network.

The Autodiscovery capability in Network Updater finds all of your Canopy network elements. This comprehensive discovery

- ensures that, when you intend to execute a script against *all* elements, the script is indeed executed against *all* elements.
- maintains master lists of elements (element groups) against which you selectively execute scripts.

The following scripts are included with CNUT:

- AP Data Import from BAM
- AP Data Export to BAM
- Set Autoupdate Address on APs
- Set SNMP Accessibility
- Reset Unit

25.5 SOFTWARE DEPENDENCIES FOR CNUT

CNUT functionality requires

- one of the following operating systems
  - Windows 2000
  - Windows XP
  - Red Hat Linux 9
  - Red Hat Enterprise Linux Version 3
- Java Runtime Version 1.4.2 or later
- Perl 5.8.0 or ActivePerl 5.8.3 software or later
- Canopy System Release 4.1 or later

25.6 CNUT DOWNLOAD

CNUT can be downloaded together with each Canopy system release that supports CNUT. Software for these Canopy system releases is packaged on the Canopy Support web page as either

- a `.zip` file for use without the CNUT application.
- a `.pkg` file (for example, `CANOPY4.2_P1.9_DES.pkg`) that the CNUT application can open.

26 INTERPRETING SYSTEM LOGS

26.1 INTERPRETING MESSAGES IN THE EVENT LOG PAGE

Each line of the Event Log web page begins with a time and date stamp. However, some of these lines wrap as a combined result of window width, browser preferences, and line length.

26.1.1 Time and Date Stamp

The time and date stamp reflect either

- GPS time and date directly or indirectly received from the CMM.
- the running time and date that you have set in the Time & Date web page.

NOTE:
In the Time & Date web page, if you have left any time field or date field unset and clicked the **Set Time and Date** button, then the time and date default to 00:00:00 UT : 01/01/00.

A reboot causes the preset time to pause or, in some cases, to run in reverse. Additionally, a power cycle resets the running time and date to the default 00:00:00 UT : 01/01/00. Thus, whenever either a reboot or a power cycle has occurred, you should reset the time and date in the Time & Date web page of any module that is not set to receive sync.

26.1.2 Event Log Data Collection

The collection of event data continues through reboots and power cycles. When the buffer allowance for event log data is reached, the system adds new data into the log and discards an identical amount of the oldest data.

Each line that contains the expression WatchDog flags an event that was both

- considered by the system software to have been an exception
- recorded in the *preceding* line.

Conversely, a Fatal Error() message flags an event that is recorded in the *next* line. Some exceptions and fatal errors may be significant and require either operator action or technical support.

An example portion of Event Log data is displayed in Figure 118. In this figure (unlike in the Event Log web page)

- lines are alternately highlighted to show the varying length of wrapped lines.
- the types of event messages (which follow the time and date stamps and the file and line references) are underscored as quoted in Table 60 and Table 61.

System Event Log

01:25:32 UT : 12/23/03 : File httptask.c : Line 616 **Reboot from Webpage.**
01:25:14 UT : 12/23/03 : File C:/ISIPPC/pssppc.250/bsps/devices/whisp/syslog.c : Line 906 **System Reset Exception -- External Hard Reset WatchDog** Cur ExtInt 25 Max ExtInt 163 Cur DecInt 22 Max DecInt 174 Cur Sync 0 Max Sync 1 Cur LED 0 Max LED 1 Cur EthXcvr 0 Max EthXcvr 1 Cur FEC 0 Max FEC 30 Cur FPGA 0 Max FPGA 1 Cur FrmLoc 25 Max FrmLoc 133 AAState 0
01:25:14 UT : 12/23/03 : File root.c : Line 840 ******System Startup******
01:25:14 UT : 12/23/03 : File root.c : Line 845 **Software Version** : CANOPY4.1 Nov 04 2003 10:38:27 AP-DES
01:25:15 UT : 12/23/03 : File root.c : Line 849 **Software Boot Version** : CANOPYBOOT 1.1
01:25:15 UT : 12/23/03 : File root.c : Line 853 **FPGA Version** : 06240308
01:25:15 UT : 12/23/03 : File root.c : Line 857 **FPGA Features** : DES
13:43:40 UT : 12/09/03 : File C:/ISIPPC/pssppc.250/bsps/devices/whisp/uplinkap.c : Line 622 **FatalError()**
13:04:22 UT : 12/30/03 : File C:/ISIPPC/pssppc.250/bsps/devices/whisp/syslog.c : Line 502 **System Log Cleared**
12:55:38 UT : 01/12/04 : File jbistub.c : Line 598 **PowerOn reset from Telnet command line.**
13:23:43 UT : 12/09/03 : File C:/ISIPPC/pssppc.250/bsps/devices/whisp/uplinkap.c : Line 620 **Expected LUID** = 6 Actual LUID = 7 BGP Count = 0
14:44:47 UT : 12/30/03 : File gps.c : Line 801 **GPS Date/Time Set**
00:40:06 UT : 01/30/04 : File C:/ISIPPC/pssppc.250/bsps/devices/whisp/syslog.c : Line 958 **Machine Check Exception** - Task: BDMT IP:20202020 Data Access Address: 8A2649E7 STACK Current:00ACF2F0 Init:00ACF400 Size:00001001
23:52:13 UT : 12/03/03 : File C:/ISIPPC/pssppc.250/bsps/devices/whisp/rf.c : Line 2261 **Aquired GPS Sync Pulse.**
17:53:21 UT : 01/26/04 : File C:/ISIPPC/pssppc.250/bsps/devices/whisp/rf.c : Line 2377 **Loss of GPS Sync Pulse.**

Figure 118: Example block of Event Log page data

26.1.3 Messages that Flag Abnormal Events

The messages listed in Table 60 flag abnormal events and, case by case, may signal the need for corrective action or technical support. See Troubleshooting on Page 376.

Table 60: Event Log messages for abnormal events

Event Message	Meaning
Expected LUID = *6* Actual LUID = *7*	Something is interfering with the control messaging of the module. If your module is operating on an earlier software release, consider upgrading to Release 4.1. Also ensure that you are using shielded cables to minimize interference. Consider trying different frequency options to eliminate or reduce interference.
FatalError()	The even recorded on the line immediately beneath this message triggered the Fatal Error().
Loss of GPS Sync Pulse	Module has lost GPS sync signal.
Machine Check Exception	This is a symptom of a possible hardware failure. If this is a recurring message, begin the RMA process for the module.
RcvFrmNum = *0x00066d* ExpFrmNum = *0x000799*	Something is interfering with the control messaging of the module. If your module is operating on an earlier software release, consider upgrading to Release 4.1. Also ensure that you are using shielded cables to minimize interference. Consider trying different frequency options to eliminate or reduce interference.
System Reset Exception -- External Hard Reset	The unit lost power or was power cycled.
System Reset Exception -- External Hard Reset WatchDog	The event recorded on the preceding line triggered this WatchDog message.

26.1.4 Messages that Flag Normal Events

The messages listed in Table 61 record normal events and typically *do not* signal a need for any corrective action or technical support.

Table 61: Event Log messages for normal events

Event Message	Meaning
Acquired GPS Sync Pulse.	Module has acquired GPS sync signal.
FPGA Features	Type of encryption.
FPGA Version	FPGA (JBC) version in the module.
GPS Date/Time Set	Module is now on GPS time.
PowerOn reset from Telnet command line	Reset command was issued from a `telnet` session.

Event Message	Meaning
Reboot from Webpage	Module was rebooted from management interface.
Software Boot Version	Boot version in the module.
Software Version	Canopy release version and authentication method for the unit.
System Log Cleared	Event log was manually cleared.

26.2 INTERPRETING DATA IN THE AP EVAL DATA PAGE (SM, BHS)

The AP Eval Data web page provides information about the AP that the SM sees (or the BHM that the BHS sees). An example of such information is shown in Figure 119.

NOTE:
In Release 4.0 and later releases, the data for this page can be suppressed by the **Disable Display of AP Eval Data** selection in the **SM Scan Privacy** field of the Configuration page on the AP.

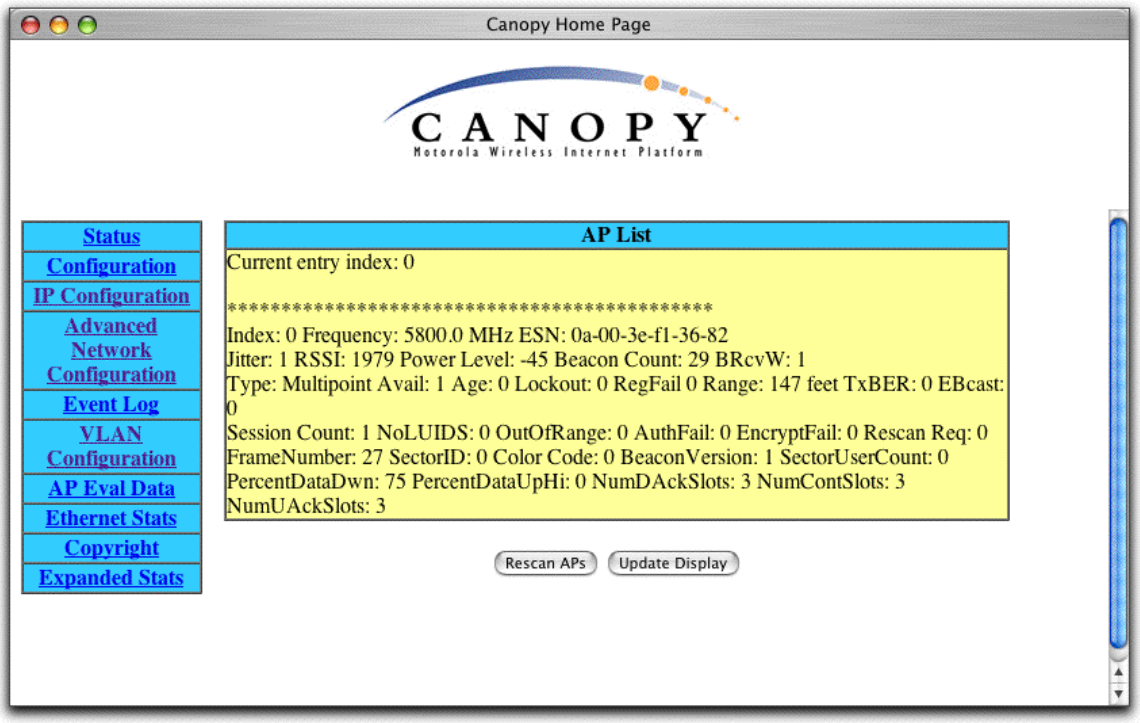

Canopy Home Page
CANOPY
Motorola Wireless Internet Platform
Status
Configuration
IP Configuration
Advanced Network Configuration
Event Log
VLAN Configuration
AP Eval Data
Ethernet Stats
Copyright
Expanded Stats
AP List
Current entry index: 0
****
Index: 0 Frequency: 5800.0 MHz ESN: 0a-00-3e-f1-36-82
Jitter: 1 RSSI: 1979 Power Level: -45 Beacon Count: 29 BRcvW: 1
Type: Multipoint Avail: 1 Age: 0 Lockout: 0 RegFail 0 Range: 147 feet TxBER: 0 EBcast: 0
Session Count: 1 NoLUIDS: 0 OutOfRange: 0 AuthFail: 0 EncryptFail: 0 Rescan Req: 0
FrameNumber: 27 SectorID: 0 Color Code: 0 BeaconVersion: 1 SectorUserCount: 0
PercentDataDwn: 75 PercentDataUpHi: 0 NumDAckSlots: 3 NumContSlots: 3
NumUAckSlots: 3
Rescan APs
Update Display

Figure 119: Example AP Eval Data screen

26.2.1 AP Eval Data Parameters

The AP Eval Data page provides the following parameters that can be useful to manage and troubleshoot a Canopy system:

Index

This field displays the index value that the Canopy system assigns (for only this page) to the AP where this SM is registered (or to the BHM to which this BHS is registered).

Frequency

This field displays the frequency that the AP or BHM transmits.

ESN

This field displays the MAC address (electronic serial number) of the AP or BHM.

Jitter

This field displays the last jitter value that was captured between this SM and the AP (or between this BHS and the BHM).

Range

This field displays the distance in feet for this link. To derive the distance in meters, multiply the value of this parameter by 0.3048.

Session Count

This field displays how many times this SM (or BHS) has gone into and out of session with the AP (or BHM). If this number is particularly large, a problem may exist in the link (for example, improper line of sight or interference).

Sector ID

This field displays the value of the **Sector ID** field that is provisioned for the AP or BHM.

Color Code

This field displays the value of the **Color Code** field that is provisioned for the AP or BHM.

Sector User Count

This field displays how many SMs are registered on the AP.

Rescan APs

You can click this button to force the SM or BHS to rescan for the frequencies that are selected in the Configuration page. (See Custom RF Frequency Scan Selection List on Page 208.) This module will then register to the AP or BHM that provides the best results for RSSI, Jitter, and number of registered modules.

26.3 INTERPRETING DATA IN THE SESSIONS PAGE (AP, BHM)

An example of the Sessions page is displayed in Figure 120.

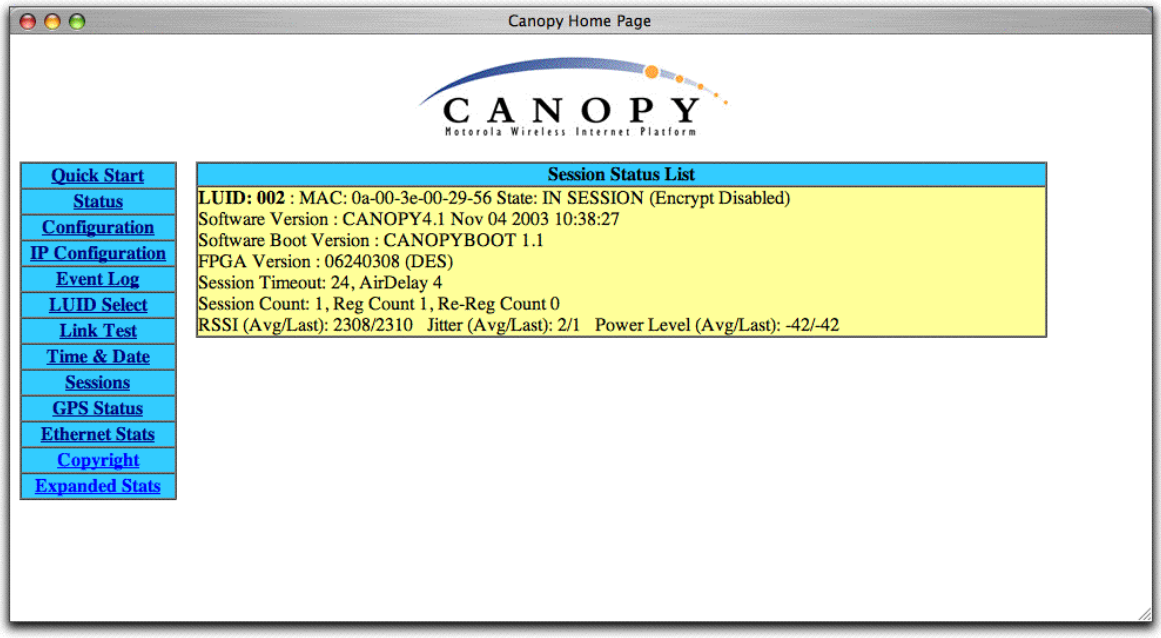


Figure 120: Example Sessions page data

The Session web page provides information about each SM that has registered to the AP (or about the BHS that has registered to the BHM). This information is useful for managing and troubleshooting a Canopy system.

26.3.1 Sessions Parameters

The Sessions page provides the following parameters.

LUID

This field displays the LUID (logical unit ID) of the SM or BHS. The first module that registers is assigned an LUID of 2. Each successive module that registers is assigned the next successively higher number. A module that loses registration and then regains registration retains the originally assigned LUID.

> *NOTE:*
> The LUID association is lost when a power cycle of the AP or BHM occurs.

MAC

This field displays the MAC address (or electronic serial number) of the SM or BHS.

State

This field displays the current status of the SM or BHS as either

- **IN SESSION** to indicate that the SM or BHS is currently registered.
- **IDLE** to indicate that the SM or BHS was registered, but now is not.

Software Version

This field displays the software release that operates on the SM or BHS, the release date of the software, the time, and whether the module is secured by DES or AES encryption (see Encrypting Canopy Radio Transmissions on Page 296). When requesting technical support, provide the information from this field.

An unpopulated **Software Version** parameter indicates a version earlier than Version 3.1.

Software Boot Version

This field indicates the CANOPYBOOT version number.

FPGA Version

This field displays the version of FPGA that runs on the SM or BHS. An unpopulated FPGA Version parameter indicates that a version earlier than Version 082002 runs on the SM or BHS.

Session Timeout

This field indicates the maximum interval in hours that the SM or BHS may sustain a single session.

AirDelay

This field displays the distance of the link. To derive the distance in meters, multiply the displayed number by 0.3048. To derive the distance in feet, multiply the displayed number by 49.

Session Count

This field displays how many sessions the SM or BHS has had. If the number of sessions is far greater than the number that other registered modules have had, then this SM or BHS may have an installation problem.

Reg Count

This field displays how many registration request messages the AP or BHM has received from the module. If the number of these messages is far greater than the number from other registered modules, then this SM or BHS may have an installation problem.

Re-Reg Count

This field displays how many registration request messages the AP or BHM has received from the module that is already in session. If the number of these messages is far greater than the number from other modules that are both registered and in session, then this SM or BHS may have an installation problem.

RSSI (Avg/Last)

This field displays the average and the latest RSSI (received signal strength indicator) value for the SM or BHS.

Jitter (Avg/Last)

This field displays the average and the latest jitter value for the SM or BHS.

Power Level (Avg/Last)

This field displays the average and the latest power level set for the SM or BHS.

26.4 INTERPRETING DATA IN THE GPS STATUS PAGE (AP, BHM)

An example of the GPS Status screen is displayed in Figure 121.

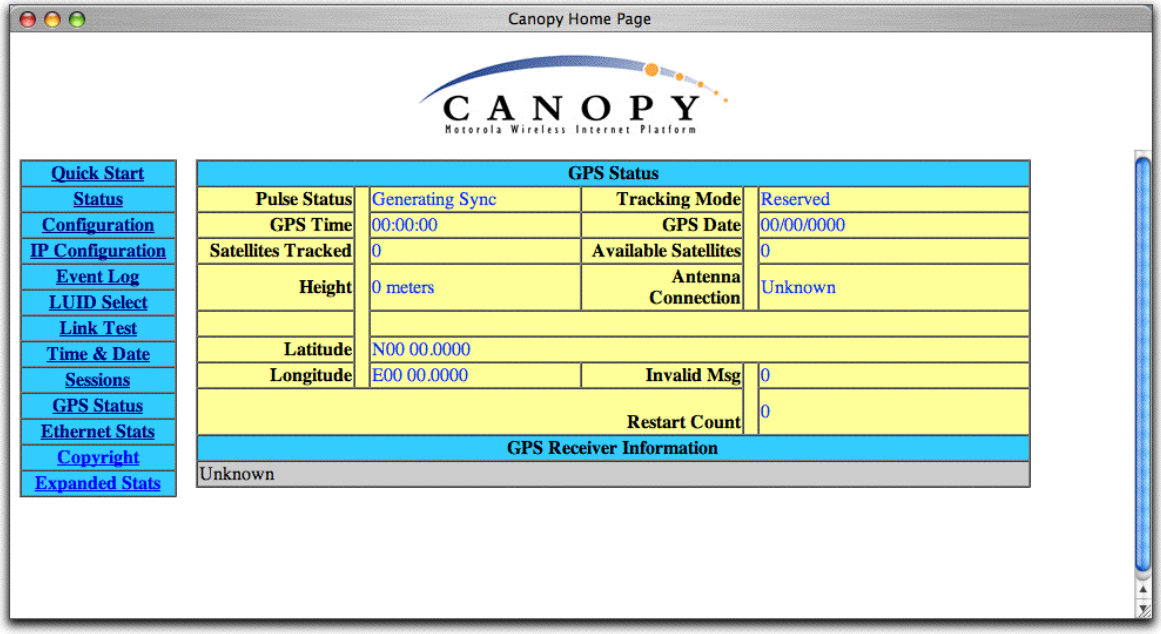


Figure 121: GPS Status screen

If the AP or BHM is configured to **Sync to Received Signal (Power Port)** and is connected to a CMMmicro, or is configured to **Sync to Received Signal (Timing Port)** and is connected to a CMM2, then the GPS Status web page provides information about satellites that the module sees and tracks. See Sync Input on Page 190.

This page also displays the state of the antenna in the **Antenna Connection** field as

- Unknown—Shown for early CMM2s. Also shown for later CMM2s and CMMmicros where the connection is not working, for an unknown reason.
- OK—Shown for later CMM2s where no problem is detected in the signal.
- Overcurrent—Indicates a coax cable or connector problem.
- Undercurrent—Indicates a coax cable or connector problem.

This information may be helpful in a decision of whether to climb a tower to diagnose a perceived antenna problem.

26.5 INTERPRETING DATA IN THE ETHERNET STATS PAGE (ALL)

The Ethernet Stats web page reports TCP throughput and error information for the Ethernet connection of the module.

26.5.1 Ethernet Stats Parameters

The Ethernet Stats page provides the following parameters.

inoctets count

This field displays how many octets were received on the interface, including those that deliver framing information.

inucastpkts count

This field displays how many inbound subnetwork-unicast packets were delivered to a higher-layer protocol.

innucastpkts count

This field displays how many inbound non-unicast (subnetwork-broadcast or subnetwork-multicast) packets were delivered to a higher-layer protocol.

indiscards count

This field displays how many inbound packets were discarded without errors that would have prevented their delivery to a higher-layer protocol. (Some of these packets may have been discarded to increase buffer space.)

inerrors count

This field displays how many inbound packets contained errors that prevented their delivery to a higher-layer protocol.

inunknownprotos count

This field displays how many inbound packets were discarded because of an unknown or unsupported protocol.

outoctets count

This field displays how many octets were transmitted out of the interface, including those that deliver framing information.

outucastpkts count

This field displays how many packets for which the higher-level protocols requested transmission to a subnetwork-unicast address. The number includes those that were discarded or not sent.

outnucastpkts count

This field displays how many packets for which the higher-level protocols requested transmission to a non-unicast (subnetwork-broadcast or subnetwork-multicast) address. The number includes those that were discarded or not sent.

outdiscards count

This field displays how many outbound packets were discarded without errors that would have prevented their transmission. (Some of these packets may have been discarded to increase buffer space.)

outerrrors count

This field displays how many outbound packets contained errors that prevented their transmission.

RxBabErr

This field displays how many receiver babble errors occurred.

EthBusErr

This field displays how many Ethernet bus errors occurred on the Ethernet controller.

CRCError

This field displays how many CRC errors occurred on the Ethernet controller.

RxOverrun

This field displays how many receiver overrun errors occurred on the Ethernet controller.

Late Collision

This field displays how many late collisions occurred on the Ethernet controller. A normal collision occurs during the first 512 bits of the frame transmission. A collision that occurs after the first 512 bits is considered a late collision.

IMPORTANT!

A late collision is a serious network problem because the frame being transmitted is discarded. A late collision is most commonly caused by a mismatch between duplex configurations at the ends of a link segment.

RetransLimitExp

This field displays how many times the retransmit limit has expired.

TxUnderrun

This field displays how many transmission-underrun errors occurred on the Ethernet controller.

CarSenseLost

This field displays how many carrier sense lost errors occurred on the Ethernet controller.

26.6 INTERPRETING DATA FROM EXPANDED STATS

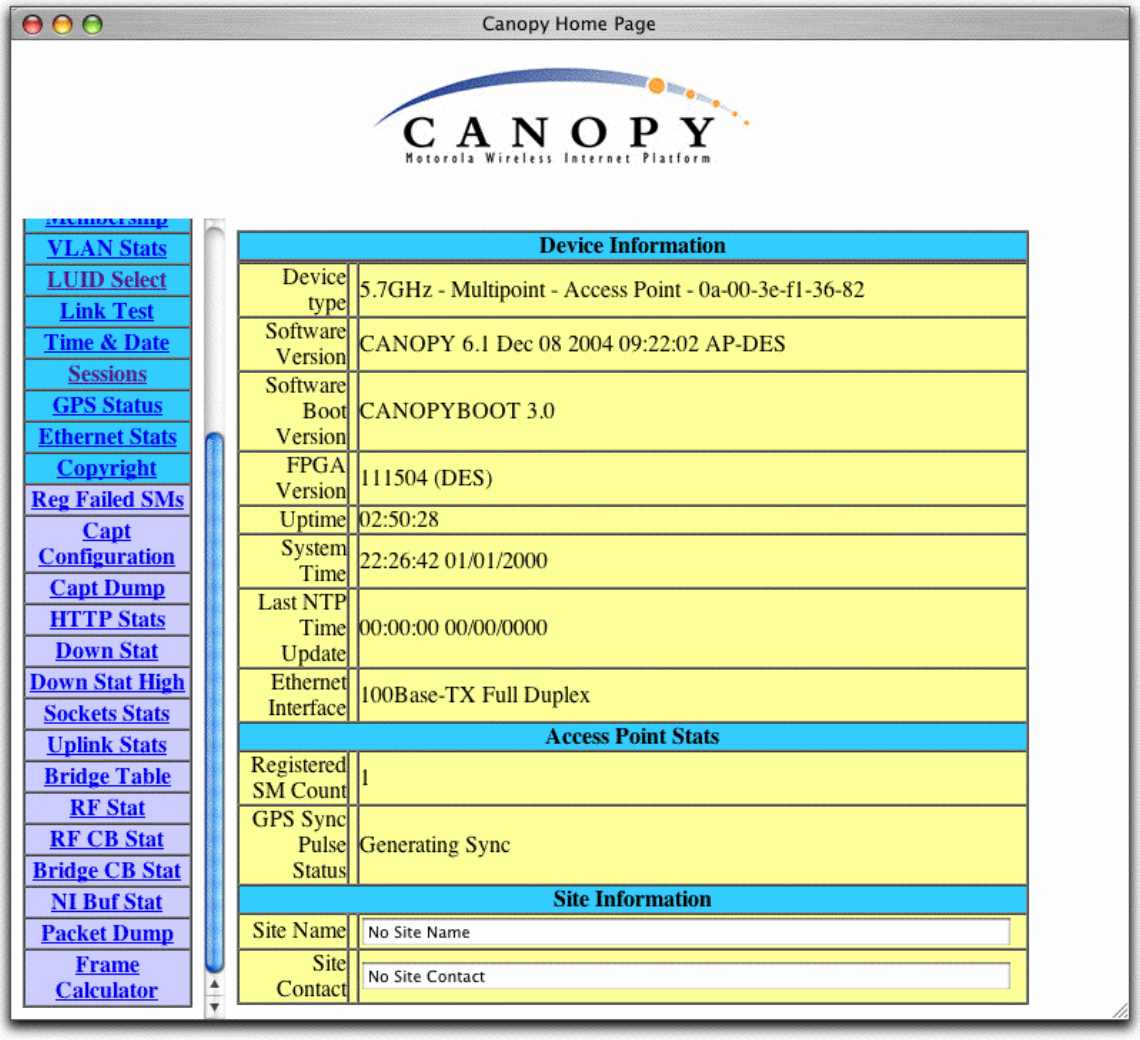


Figure 122: Status screen, AP, after Expanded Stats is selected

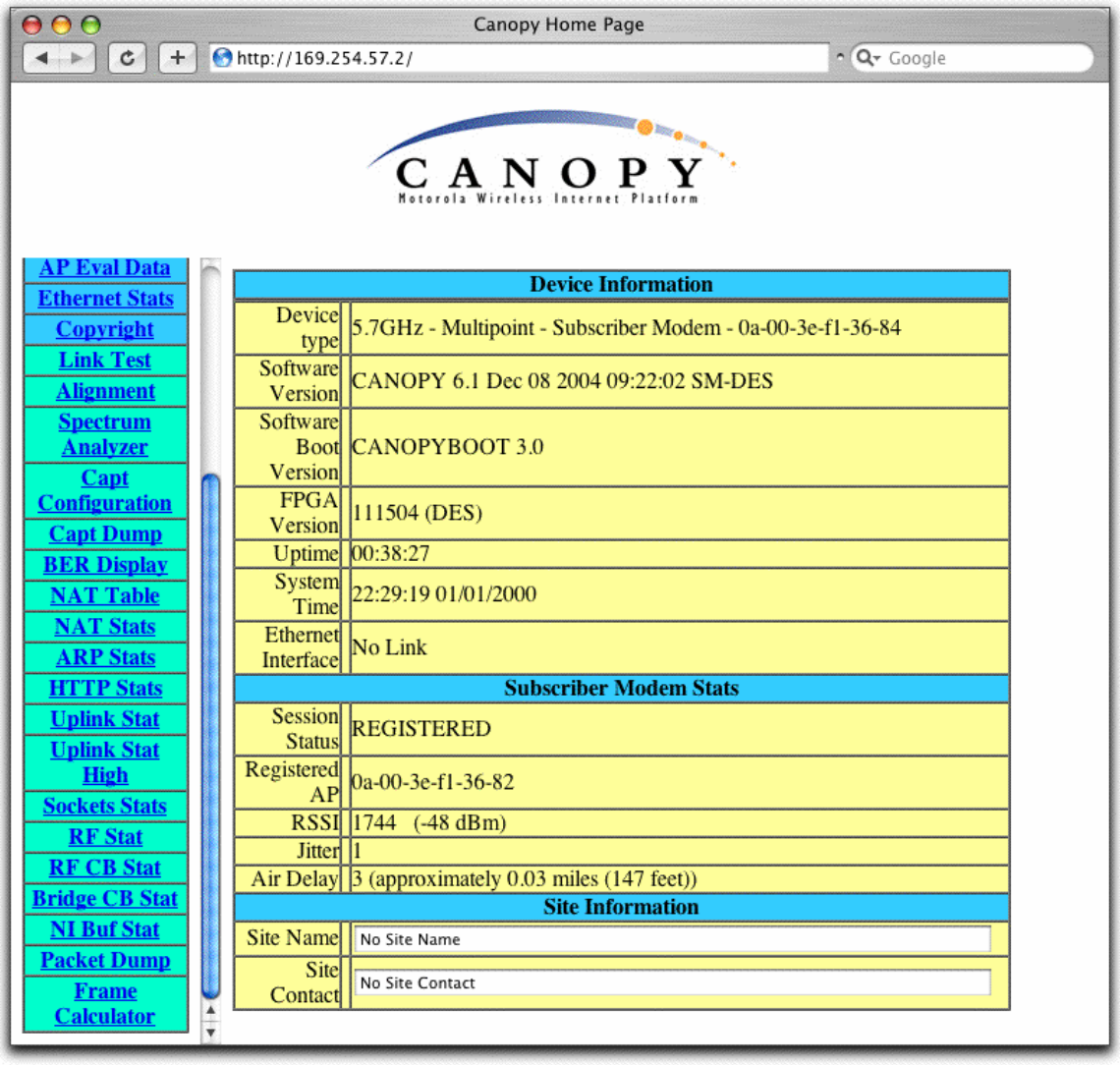


Figure 123: Status Screen, SM, after Expanded Stats is selected

When you click the **Expanded Stats** button on the left side of any earlier-described module web page

- the Status page data in the AP or BHM is expanded to include the following radio fields:
  - **Radio Slicing Value**
  - **Radio Transmit Gain Setting**

  and the following Frame Configuration Information fields:
  - **Data Slots Down**
  - **Data Slots Up**
  - **NumUAck Slots** (and **Number Hi Priority**)
  - **NumDAck Slots** (and **Number Hi Priority**)
  - **NumCtl Slots** (and **Number Hi Priority**)

- the Status page in the SM or BHS is expanded to include the following radio fields:
  - **Radio Slicing Value**
  - **Radio Transmit Gain Setting**
  - **Power Level**
  - **LUID**
  - **IP Address**
  - **Registration Grant Status**
  - **Sustained Uplink Data Rate**
  - **Uplink Burst Allocation**
  - **Sustained Downlink Data Rate**
  - **Downlink Burst Allocation**

  and the following Frame Configuration Information fields:
  - **Data Slots Down**
  - **Data Slots Up**
  - **NumUAck Slots** (and **Number Hi Priority**)
  - **NumDAck Slots** (and **Number Hi Priority**)
  - **NumCtl Slots** (and **Number Hi Priority**)
- the link menu on the left side of the page is expanded to include links to the following additional web pages:

Alignment Page (SM, BHS)	*RF Cal Log Page (All)*
AP Ses Log Page (AP, BHM)	*RF CB Stat Page (All)*
AP Update Log Page (AP, BHM)	*RF Scan Log Page (SM, BHS)*
BER Display Page (SM, BHS)	*RF Session Log Page (All)*
Bridge CB Stat Page (All)	*RF Stat Page (All)*
Bridge Table Page (All)	*RF Sync Log Page (All)*
Capt Configuration	*SM CCenter Log Page (SM, BHS)*
Capt Dump	*SM Ses Log Page (SM, BHS)*
Downlink Log Page (AP, BHM)	*SM Sync Log Page (SM, BHS)*
Downlink Log High Page (AP, BHM)	*SM Update Log Page (SM, BHS)*
Frame Calculator	*Socket Stats Page (All)*
HTTP Stats Page (All)	Spectrum Analyzer Page (SM, BHS)
Link Test Page (All)	*Update Sess Log Page (AP, BHM)*
NI Buf Stat Page (All)	*Uplink Stats Page (All)*
Packet Dump Page (All)	*Uplink Stat Hi Page (SM, BHS)*
Reg Failed SMs Page (AP, BHM)	

NOTE:
The pages italicized in the above list are for viewing under the guidance of Canopy Technical Support.

When you have clicked the **Expanded Stats** button, you cannot toggle the interface back (to hide these additional web pages and Status data) by clicking the button again. You can click only the **Back** button of your browser to do so.

26.6.1 Alignment Page (SM, BHS)

An example of the Alignment screen is displayed in Figure 112 on Page 280.

Modes

The Alignment web page provides tools to assist in the alignment of an SM to an AP (or BHS to a BHM). Whether and how these tools operate depends on the mode that you invoke. The following modes are available:

- Normal Aiming Mode
- RSSI Only Aiming Mode
- Operating Mode

Regardless of the mode that you select to align the module, you must achieve all of the following indications for an acceptable link between the modules:

- RSSI greater than 700
- jitter value between 0 and 4 in Release 4.0 and later releases or between 5 and 9 in any earlier release
- uplink efficiency greater than 90%
- downlink efficiency greater than 90%

IMPORTANT!
If any of these values is not achieved, a link can be established but manifest occasional problems. In Release 4.0 and late releases, RSSI measurement is more consistent and jitter control is improved.

In either aiming mode, you must either set the Alignment page to automatically refresh or repeatedly click the **Enable Aiming Mode** button to keep current data displayed as the module is moved. After 15 minutes in an aiming mode, the module is automatically reset into the Operating Mode.

Normal Aiming Mode

In the Normal Aiming Mode

- the screen displays the RSSI level and the jitter value.
- the five left-most LEDs in the module act as a bar graph that indicates the best achieved RSSI level and jitter value when the greatest number of LEDs is lit. (The colors of the LEDs are not an indication in this mode.)

To invoke the Normal Aiming Mode

1. ensure that the **Disabled** button on the **RSSI Only Mode** line is checked.
2. click the **Enable Aiming Mode** button. (The aiming procedure is described on Page 280.)

RSSI Only Aiming Mode

In the RSSI Only Aiming Mode, the screen displays the signal strength based on the amount of energy in the selected frequency, regardless of whether the module has registered. This mode simplifies the aiming process for long links, such as where the module is mounted to a Canopy Passive Reflector.

To invoke the RSSI Only Aiming Mode

1. select the frequency of the AP in the Configuration Page of the SM. See Custom RF Frequency Scan Selection List on Page 208.
2. click the **Enable** button on the **RSSI Only Mode** line of the Alignment page.
3. click the **Enable Aiming Mode** button. (The aiming procedure is described on Page 280.)

26.6.2 BER Display Page (SM, BHS)

An example of the BER Results screen is displayed in Figure 124.

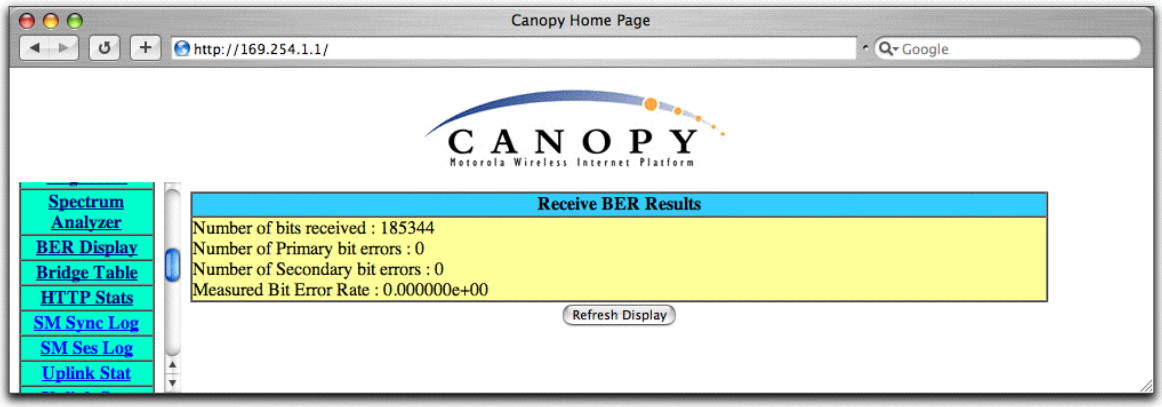


Figure 124: BER Results screen

BER Display

This page displays the current bit error rate in the link, but only if the AP or BHM is configured to send the BER stream.

The value in the **Measured Bit Error Rate** field represents the BER at the moment of the last browser refresh. To keep the value of this field current, either repeatedly click the **Refresh Display** button or set the screen to automatically refresh.

BER Results

The link is acceptable if the value of this field is less than 10^{-4}. If the BER is greater than 10^{-4}, re-evaluate the installation of both modules in the link.

26.6.3 Bridge Table Page (All)

An example of the Bridge Table screen is displayed in Figure 125.

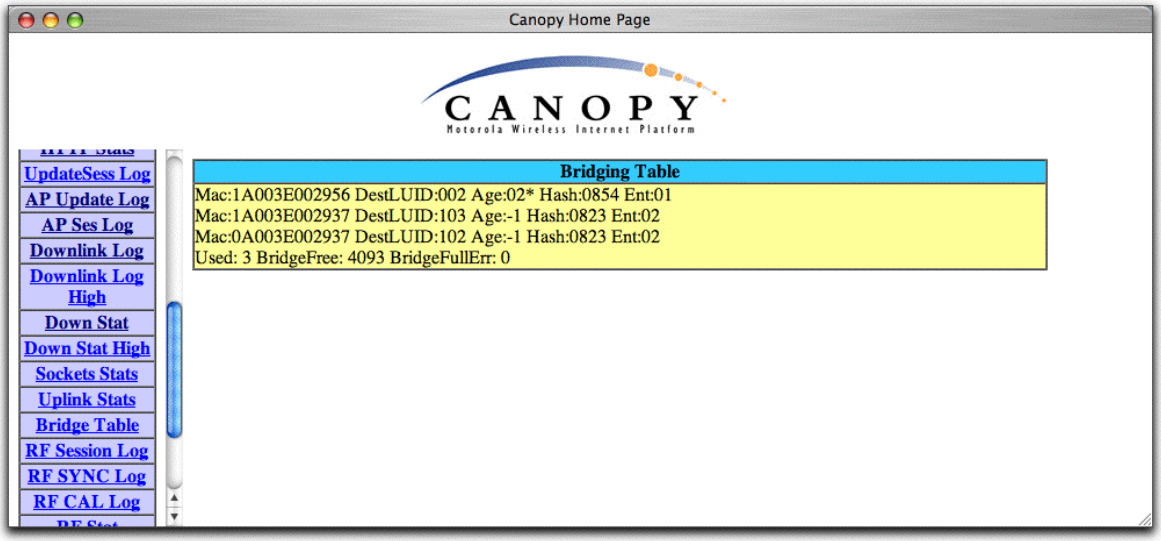


Figure 125: Bridge Table screen

If NAT (network address translation) is not active on the SM, then the Bridge Table web page provides the MAC address of all devices that are attached to registered SMs (identified by LUIDs). The bridging table allows the AP to send data to the correct SM.

26.6.4 Frame Calculator Page

Canopy avoids self-interference by syncing collocated APs (so they begin each transmission cycle at the same time) and requiring that collocated APs have the same transmit/receive ratio (so they stop transmitting and start receiving at the same time). This ensures that, at any instant, they are either all receiving or all transmitting.

This avoids, for example, the problem of one AP attempting to receive from a distant SM, while a nearby AP is transmitting and overpowering the signal from the distant SM. Parameters that affect transmit/receive ratio include range, slots, downlink data percentage, and high priority uplink percentage. In releases earlier than 6.1, Canopy ensured that APs in a cluster had the same transmit/receive ratio by requiring that all these parameters be set the same. Release 6.1, introduces a new frame structure for hardware scheduler than for software scheduler, but the rule remains: to have all collocated APs have the same transmit/receive ratio. Additional engineering is needed for setting the parameters in a mixed cluster – one running APs on both hardware and software schedulers.

Release 6.1 and later includes a frame calculator to help do this. The operator inputs various AP settings into the calculator, and the calculator outputs many details on the frame including the **Uplink Rec SQ Start**. This calculation should be done for each AP that has different settings. Then the operator varies the **Downlink Data** percentage in each calculation until the calculated **Uplink Rec SQ Start** for all collocated APs is within 300 time bits. The frame calculator is available on any module running Release 6.1 or

later by clicking on Expanded Stats in the navigation column, then clicking on Frame Calculator (at the bottom of the expanded navigation column).

The calculator does not use data on the module or populate new data. It is merely a convenience application running on the module. For this reason, you can use any module running Release 6.1 or later to do the calculations for any AP. Running the calculator on the AP in question is not necessary.

Figure 126 and Figure 127 show how to use the calculator to discover values of **Downlink Data** percentage that will put all the **Uplink Rcv SQ Start** values within the required 300 time bits.

IMPORTANT!

APs with slightly mismatched transmit/receive ratios and low levels of data traffic may see little effect on throughput. As the data traffic increases, the impact of mismatched transmit/receive ratios will increase. This means that a system that wasn't tuned for collocation may work fine at low traffic levels, but have issues at higher traffic level. The conservative practice is to tune for collocation from the beginning, and prevent future problems as sectors are built out and traffic increases.

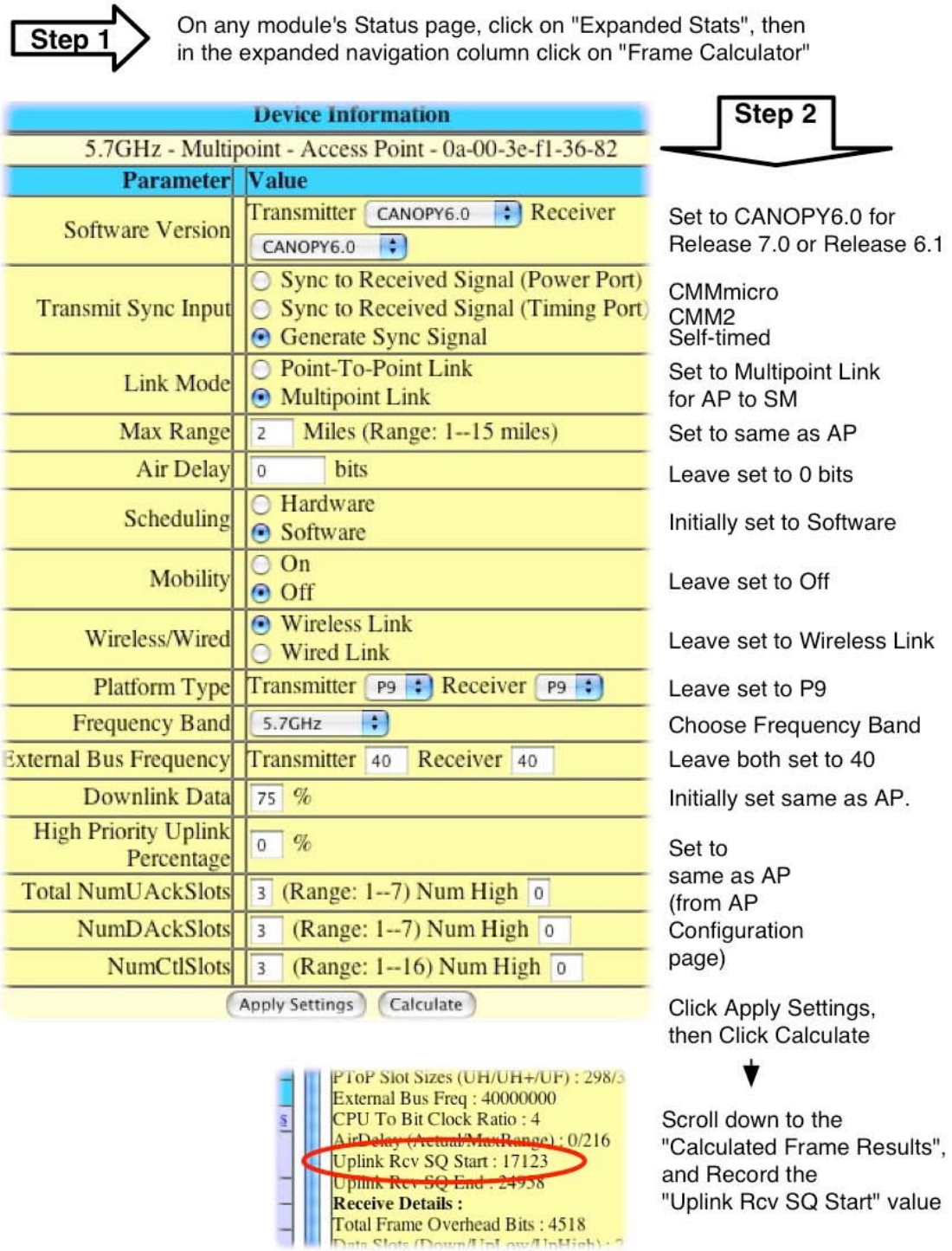


Figure 126: Discovering downlink data percentages for collocation

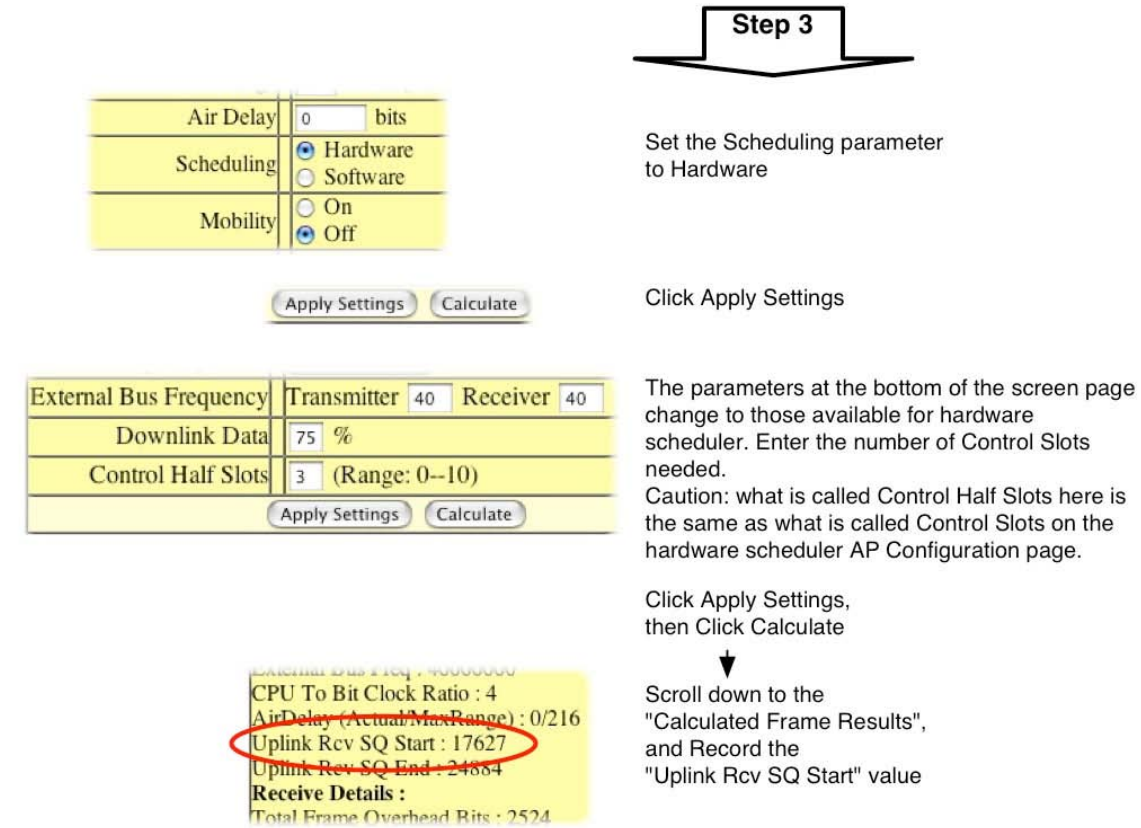

Step 3
Air Delay 0 bits
Scheduling Hardware Software
Mobility On Off
Set the Scheduling parameter to Hardware
Apply Settings Calculate
Click Apply Settings
External Bus Frequency Transmitter 40 Receiver 40
Downlink Data 75 %
Control Half Slots 3 (Range: 0--10)
Apply Settings Calculate
The parameters at the bottom of the screen page change to those available for hardware scheduler. Enter the number of Control Slots needed.
Caution: what is called Control Half Slots here is the same as what is called Control Slots on the hardware scheduler AP Configuration page.
Click Apply Settings, then Click Calculate
CPU To Bit Clock Ratio : 4
AirDelay (Actual/MaxRange) : 0/216
Uplink Rcv SQ Start : 17627
Uplink Rcv SQ End : 24884
Receive Details :
Total Frame Overhead Bits : 2524
Scroll down to the "Calculated Frame Results", and Record the "Uplink Rcv SQ Start" value
Step 4
All the "Uplink Rcv SQ Start" values of collocated APs must be within a 300 time bit range.
Use the calculator to iterate, changing the "Downlink Data %" to get values for all APs within 300 time bits.
Now leave the Frame Calculator and go to each AP's Configuration page. Use the discovered Downlink Data percentages to set the appropriate AP's Downlink Data % on each AP's Configuration page.

Figure 127: Discovering downlink data percentages for collocation, continued

26.6.5 Link Test Page (All)

An example of the Link Capacity Test screen is displayed in Figure 128.

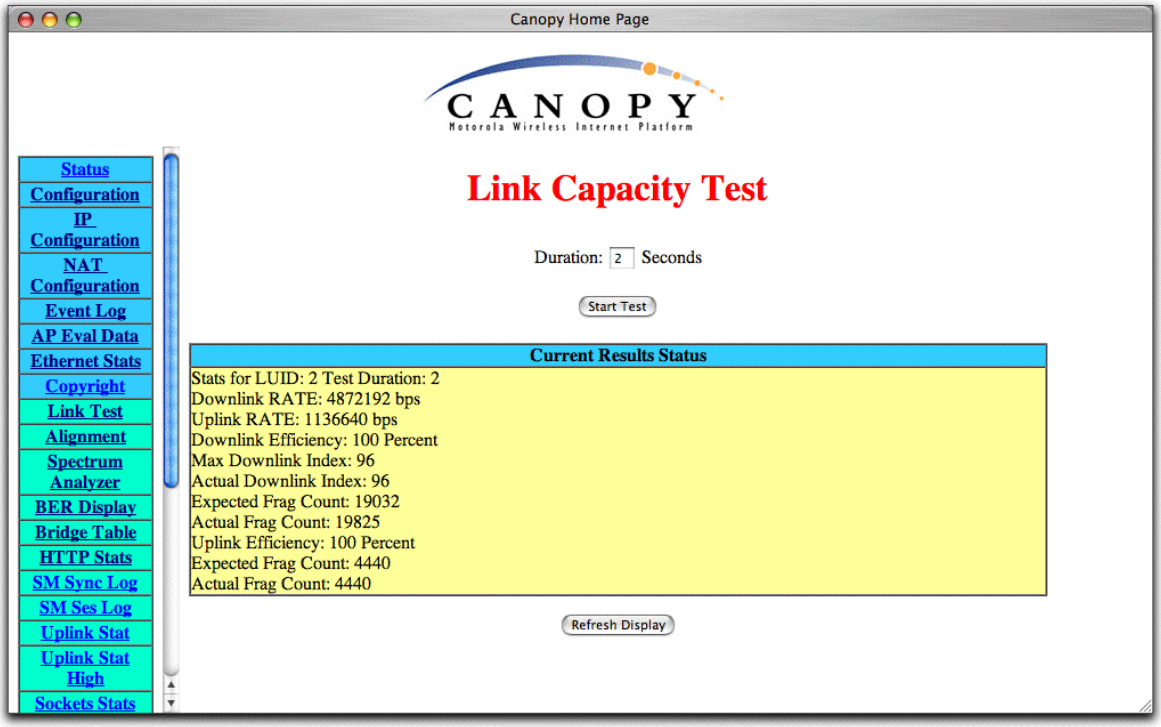


Figure 128: Link Test screen

The Link Capacity Test page allows you to measure the throughput and efficiency of the RF link between two Canopy modules. To test a link using this page, perform the following steps:

1. Enter into the **Duration** field how long (in seconds) the RF link should be tested.
2. Click the **Start Test** button.
3. Click the **Refresh Display** button (if the web page is not set to automatically refresh).
4. View the results of the test.

Key Link Capacity Test Fields

The key fields in the test results are

- **Downlink RATE**, expressed in bits per second
- **Uplink RATE**, expressed in bits per second
- **Downlink Efficiency**, expressed as a percentage
- **Uplink Efficiency**, expressed as a percentage

Capacity Criteria for the Link

A Canopy system link is acceptable only if the efficiencies of the link test are greater than 90% in both the uplink and downlink direction. Whenever you install a new link, execute a link test to ensure that the efficiencies are within recommended guidelines.

26.6.6 Reg Failed SMs Page (AP, BHM)

An example of the Reg Failed SMs screen is displayed in Figure 129.

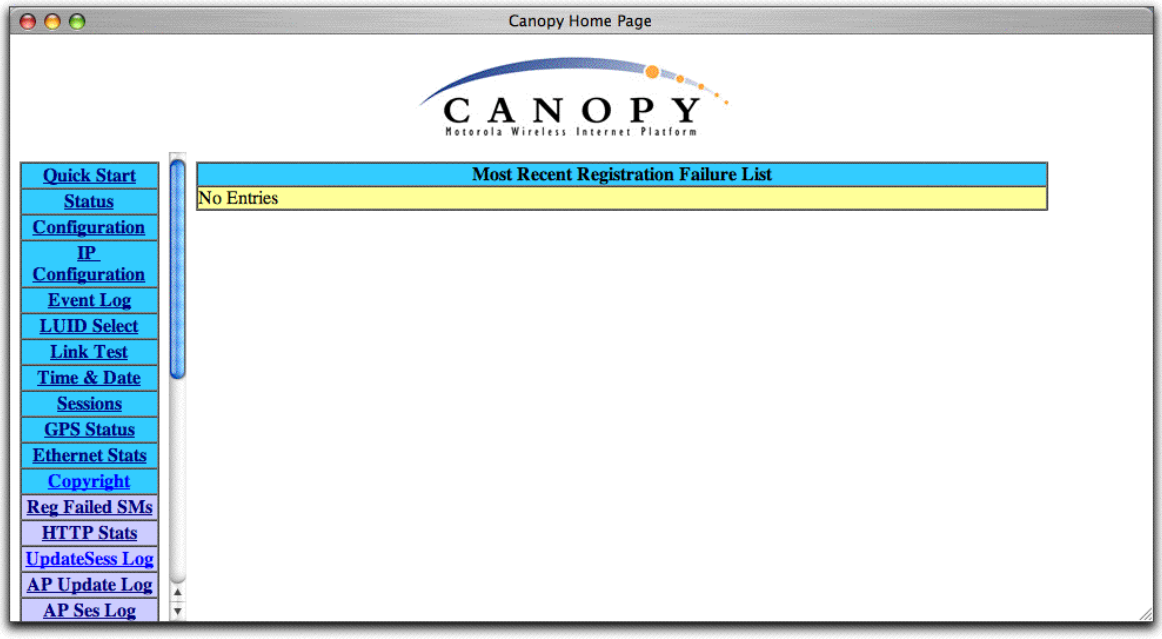


Figure 129: Reg Failed SMs screen

The Reg Failed SMs web page identifies SMs (or BHSs) that have recently attempted and failed to register to this AP (or BHM).

26.6.7 Spectrum Analyzer Page (SM, BHS)

See Monitoring the RF Environment on Page 285.

27 MAINTAINING YOUR CANOPY SOFTWARE

Canopy provides release compatibility information and caveats about each release.

27.1 HISTORY OF SYSTEM SOFTWARE UPGRADES

Canopy currently supports System Releases 3.2, 4.0, 4.1, and 4.2.

27.1.1 System Release 3.1.5 Features

Canopy System Release 3.1.5 introduced the following features:

- 5.7-GHz Module Support
- Enhanced Alignment Mode
- BHM Bridge Changes
- Bridge Table from 256 to 4096 Entries
- Configurable Bridge Table Timeout
- Data Encryption Standard (DES) Encryption
- Default Downlink Percentages: AP 75%, BH 50%
- Public IP Access for SM
- Public IP Access for BHS
- Customer Logo on Web-based Interface
- BH Configurable for Master or Slave
- Passwords on FTP and Telnet Sessions
- Default Router Change for BHS
- Default Router Change for SM
- GPS Sync Protection

27.1.2 System Release 3.2 Features and Fixes

Canopy System Release 3.2 introduced the following features:

- Disable SM Ethernet Interface
- Canopy Enterprise MIB

Canopy Software Release 3.2 also introduced the following fixes:

- Oversized (Up to 1532 Bytes) Ethernet Frame Fix
- BH Hash Table Fix

27.1.3 System Release 4.0 Features

Canopy System Release 4.0 introduced the following features:

- 5.7-GHz Module ISM Frequencies Support
- Advanced Encryption Standard (AES) Encryption
- Audible Alignment Tone
- BH Authentication

- Transmit Frame Spreading
- GPS Antenna Connection Status
- Improved Jitter Control
- Updated Canopy Enterprise MIB
- 20-Mbps BH to 10-Mbps BH Modulation
- Power Level Measurement
- Display Registered AP
- Registration Failed SM List
- No Remote Access
- Improved Received Signal Strength Indicator (RSSI)
- SM Scan Privacy
- Extended Network with Sync

27.1.4 System Release 4.0.1 Fixes

Canopy System Release 4.0.1 introduced the following fixes:

- Bus Bandwidth Limitation Causing 20-Mbps BH Errors Fix
- 20-Mbps BH Jitter Measurement Fix

27.1.5 System Release 4.0.2 Fixes

Canopy System Release 4.0.2 introduced the following fixes:

- Audible Alignment Tone on Only SMs and BHSs Fix
- ISM State Preserved through Reset to Factory Defaults Fix

27.1.6 System Release 4.0.4 Fix

Canopy System Release 4.0.4 introduced the following fix:

- Telnet Corrupting GPS Information Fix

27.1.7 System Release 4.1 Features

Canopy System Release 4.1 introduced the following features:

- SM Auto Update
- DHCP Server and Client in SM
- Demilitarized Zone (DMZ) in SM
- Updated Canopy Enterprise MIB
- Network Address Translation (NAT) in SM
- Low Power Mode (18-dB Reduction)
- Spectrum Analyzer in SM and BHS

27.1.8 System Release 4.2.1 Features

Canopy System Release 4.2.1 introduced the following features:

- Software Limit Increase on 2.4-GHz Module (from 15 to 30 Miles)
- Settable AP Broadcast Repeat Count
- Encrypted Downlink Broadcast
- Protocol and Port Filtering
- Configurable Hyperlinked Logo
- Updated Canopy Enterprise MIB
- NAT Support for VPNs—L2TP Over IPSec
- SM and BHS Site Names in AP or BHM Sessions Page
- Graphical Spectrum Analyzer in SM and BHS
- PDA Info and Spectrum Analyzer Pages
- Telnet Commands Defined
- Web Pages Remain Scrolled
- Time & Date for APs or BHMs Connected to CMMmicro

Canopy System Release 4.2.1 also introduced the following fixes:

- BH 64-byte Packet Asynchronicity Fix
- Wrongly Reported DMZ IP Conflict with DHCP Server IP Range Fix
- SNMP Manager and SM Subnet Address Fix

27.1.9 System Release 4.2.2 Feature

Canopy System Release 4.2.2 introduced the following feature:

- 900-MHz Module (all P9) Support

27.1.10 System Release 4.2.3 Features and Fixes

Canopy System Release 4.2.3 introduced the following features:

- 5.7-GHz Module P9 Support
- New Alignment Tone for P9 Boards
- Floating Licenses for APs with Authentication
- Shorter than 32 Hex Authentication Keys Accepted
- CANOPYBOOT Version 3.0 Fix (Replaces Version 2.5)
- Dynamic Frequency Selection (DFS) for 5.7-GHz Module
- Improved Protocol and Port Filtering
- Consistent Display of FPGA as 6 digits
- Updated Canopy Enterprise MIB

Canopy System Release 4.2.3 also introduced the following fixes:

- DHCP Client Sends Lease Renewals as Unicast Fix
- DMZ Host as FTP Client Fix

27.1.11 System Release 4.2.7 Features and Fix

Canopy System Release 4.2.7 introduced the following features:

- 2.4-GHz Module P9 Support
- 5.2-GHz Module P9 Support
- 5.4-GHz Module P9 Support
- 5.4-GHz Module Dynamic Frequency Selection (DFS) for Radar
- 5.4-GHz Module Adjustable Power
- 2.4-GHz Module Adjustable Power

Canopy System Release 4.2.7 also introduced the following fix:

- Alignment Tone Fix

27.1.12 System Release 6.0 Features

Canopy System Release 6.0 introduced the following features:

- 900-MHz Module Dynamic per-SM High-priority Channel with Hardware Scheduler
- 900-MHz Module Hardware Scheduler Reduced Latency
- 900-MHz Module Spectrum Analyzer in AP
- 900-MHz Module Hardware Scheduler Increased Throughput

27.1.13 System Release 6.1 Features and Fix

Canopy System Release 6.1 introduced the following features:

- Release 6.0 Compatibility Mode for 900-MHz Module
- Committed Information Rate (CIR) with Hardware Scheduler
- Configuration Source Parameter at AP for VLAN, MIR, and CIR
- Frame Calculator for Tuning Mixed Clusters
- All Frames Adjusted for Cross-release Communications
- Dynamic per-SM High-priority Channel with Hardware Scheduler
- Reduced Latency with Hardware Scheduler
- Maximum Information Rate (MIR) Settable at SM
- 5.7-GHz Module Adjustable Power with Connectorized Antenna
- Spectrum Analyzer in AP
- Increased Throughput with Hardware Scheduler
- VLAN (802.1Q)

Canopy System Release 6.1 also introduced the following fix:

- Alignment Tone Fix

27.2 HISTORY OF CMMmicro SOFTWARE UPGRADES

Canopy currently supports CMMmicro Releases 1.0, 2.1, and 2.1.1. Release 2.1 introduced the NTP Server in CMMmicro feature. Release 2.1.1 introduced the following features:

- Telnet Support in CMMmicro for All Clients
- Telnet through Radio to CMMmicro

27.3 TYPICAL CONTENTS OF RELEASE NOTES

Canopy supports each release with software release notes. This documentation includes

- description of features that are introduced in the new release.
- problems that the new release resolves.
- known problems inherent in the new release.
- installation procedures for the new release.
- troubleshooting information for the upgrade.

27.4 TYPICAL UPGRADE PROCESS

In a typical upgrade process, proceed as follows:

1. Visit the software page of the Canopy web site.
2. Read the compatibility information and any caveats that Canopy associates with the release.
3. Read the software release notes from the web site.
4. On the basis of these, decide whether the release is appropriate for your network.
5. Download the software release and associated files.
6. Use CNUT to manage the upgrade across your network.

27.4.1 Downloading Software and Release Notes

All supported software releases, the associated software release notes document, and updated MIB files are available for download at any time from http://motorola.canopywireless.com/support_software.php. This web site also typically provides a summary of the backward compatibility and any advantages or disadvantages of implementing the release.

When you click on the release that you wish to download, you are prompted for information that identifies yourself and your organization (such as name, address, and e-mail address). When you complete and submit the form that prompts for this information, the download is made available to you.

28 BRANDING WEB PAGES

Distinctive fonts indicate

literal user input.
variable user input.
literal system responses.
variable system responses.

28.1 REBRANDING WEB PAGES TO YOUR BRAND

The web-based interface screens on each Canopy module contain the Canopy logo. A file named `canopy.jpg` generates the Canopy logo. You can replace the Canopy logo with your company logo as follows.

Procedure 44: Replacing the Canopy logo

1. Copy your custom logo file to the name `canopy.jpg` on your system.
2. Use an FTP (File Transfer Protocol) session to transfer the new `canopy.jpg` file to the module, as in the example session shown in Figure 130.

```
> ftp ModuleIPAddress
Connected to ModuleIPAddress
220 FTP server ready
Name (ModuleIPAddress:none): root
331 Guest login ok
Password: <password-if-configured>
230 Guest login ok, access restrictions apply.

ftp> binary
200 Type set to I
ftp> put canopy.jpg
ftp> quit
221 Goodbye
```

Figure 130: Example ftp session to transfer logo

3. Use a telnet session to add the new `canopy.jpg` file to the file system, as in the example session shown in Figure 131.

NOTE:
Supported telnet commands execute the following results:

- **addwebfile** adds a custom logo file to the file system.
- **clearwebfile** clears the customer logo file from the file system.
- **lsweb** lists the custom logo file and display the storage space available on the file system.

```
>telnet ModuleIPAddress

/---------\
C A N O P Y

Motorola Broadband Wireless Technology Center
(Copyright 2001, 2002 Motorola Inc.)

Login: root
Password: <password-if-configured>

Telnet+> lsweb
Flash Web files
/canopy.jpg     7867
free directory entries: 31
free file space: 56468

Telnet +> clearwebfile
Telnet+> lsweb

Flash Web files
free directory entries: 32
free file space     64336 bytes

Telnet +> addwebfile canopy.jpg
Telnet +> lsweb

Flash Web files
/canopy.jpg     7867
free directory entries: 31
free file space: 55331

Telnet +> exit
```

Figure 131: Example telnet session to change screen logo

========== **end of procedure** ==========

28.2 CONFIGURING A HYPERLINKED LOGO

In Canopy System Release 4.2 and later releases, you can import a logo into the top of any Canopy interface web page from any URL by establishing a hyperlink. This requires simple html page editing and saving the resulting page into the module as follows.

Procedure 45: Changing the hyperlinked URL for the top of Canopy web pages

1. Browse to http://*ModuleIPAddress*/top.html.
2. In the html editor of your choice, open the file `top.html`.
3. Find the expression `http://www.canopywireless.com`.
4. Change `http://www.canopywireless.com` to the URL where your chosen logo is stored.
5. Find the expression `canopy.jpg`.
6. Change `canopy.jpg` to ***`yourlogo.jpg`***.
   NOTE: The filename extension should be that of your logo file.
7. Save the file as `top.html`.
8. Use an FTP session to transfer both `top.html` and *`yourlogo.jpg`* to the module, as in the example session shown in Figure 132 below.
9. Use a telnet session to add the file *`yourlogo.jpg`* to the file system of the module, as in the example session shown in Figure 133 below.

========== **end of procedure** ==========

```
> ftp ModuleIPAddress
Connected to ModuleIPAddress
220 FTP server ready
Name (ModuleIPAddress:none): root
331 Guest login ok
Password: <password-if-configured>
230 Guest login ok, access restrictions apply.
ftp> binary
200 Type set to I
ftp> put yourlogo.jpg
ftp> put top.html
ftp> quit
221 Goodbye
```

Figure 132: Example ftp session to transfer logo and hyperlink file

```
>telnet ModuleIPAddress

/---------\
C A N O P Y

Motorola Broadband Wireless Technology Center
(Copyright 2001, 2002 Motorola Inc.)

Login: root
Password: <password-if-configured>
Telnet+> clearwebfile
Telnet+> addwebfile yourlogo.jpg
Telnet+> addwebfile top.html
Telnet+> lsweb

Flash Web files
/yourlogo.jpg 7867
/top.html 313
free directory entries: 32
free file space: 64336 bytes
Telnet+> exit
```

Figure 133: Example telnet session to add logo and hyperlink file

29 TOGGLING REMOTE ACCESS CAPABILITY

In Release 4.0 and later releases, based on your priorities for additional security and ease of network administration, you can deny or permit remote access individually to any AP, SM, or BH.

29.1 DENYING ALL REMOTE ACCESS

Wherever the No Remote Access feature is enabled (by the following procedure), physical access to the module is required for

- any change in the configuration of the module.
- any software upgrade in the module.

Where additional security is more important that ease of network administration, you can disable all remote access to a module as follows.

Procedure 46: Denying all remote access

1. Insert the override plug into the RJ-11 GPS utility port of the module.
2. Power up or power cycle the module.
3. Access the web page http://169.254.1.1/lockconfig.html.
4. Click the check box.
5. Save the changes.
6. Reboot the module.
7. Remove the override plug.
   RESULT: No access to this module is possible through HTTP, SNMP, FTP, telnet, or over an RF link.

========== **end of procedure** ==========

29.2 REINSTATING REMOTE ACCESS CAPABILITY

Where ease of network administration is more important than the additional security that the No Remote Access feature provides, this feature can be disabled as follows:

Procedure 47: Reinstating remote access capability

1. Insert the override plug into the RJ-11 GPS utility port of the module.
2. Power up or power cycle the module.
3. Access the web page http://169.254.1.1/lockconfig.html.
4. Click the check box to uncheck the field.
5. Save the changes.
6. Reboot the module.

7. Remove the override plug.
   RESULT: Access to this module is possible through HTTP, SNMP, FTP, telnet, or over an RF link.

========== **end of procedure** ==========

30 SETTING UP A PROTOCOL ANALYZER ON YOUR CANOPY NETWORK

Selection of protocol analyzer software and location for a protocol analyzer depend on both the network topology and the type of traffic to capture. However, the examples in this section are based on free-of-charge Ethereal software, which is available at http://ethereal.com/

The equipment required to set up a protocol analyzer includes:

- 1 hub
- 1 laptop computer with protocol analyzer software installed
- 2 straight-through Ethernet cables
- 1 Canopy power converter (ACPS110)

30.1 ANALYZING TRAFFIC AT AN SM

The IP address of the protocol analyzer laptop computer must match the IP addressing scheme of the SM. If the SM has DHCP enabled, then configure the laptop computer to automatically obtain an address. If DHCP is not enabled, then ensure that the laptop computer is configured with a static IP address in the same subnet as the SM.

The configuration for analyzing traffic at an SM is shown in Figure 134.

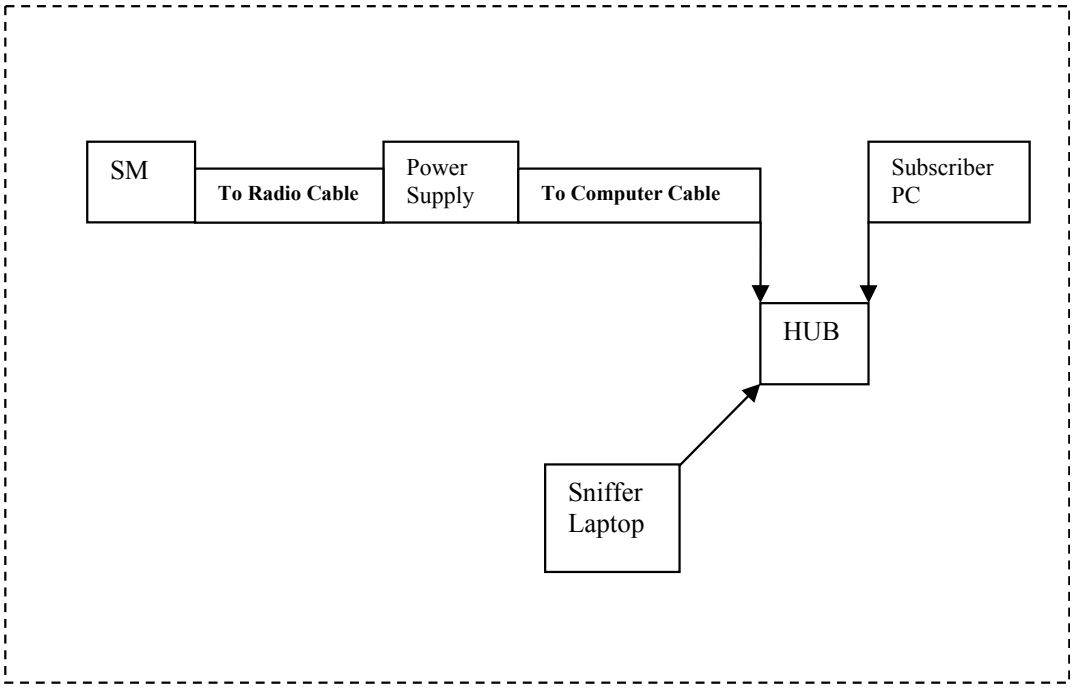


Figure 134: Protocol analysis at SM

30.2 ANALYZING TRAFFIC AT AN AP OR BH WITH NO CMM

The IP address of the protocol analyzer laptop computer must match the IP addressing scheme of the AP/BH. If the router is configured to be a DHCP server, then configure the laptop computer to automatically obtain an address. If DHCP is not enabled, then ensure that the laptop computer is configured with a static IP address in the same subnet as the AP/BH.

The configuration for analyzing traffic at an AP or BH that *is not* connected to a CMM is shown in Figure 135.

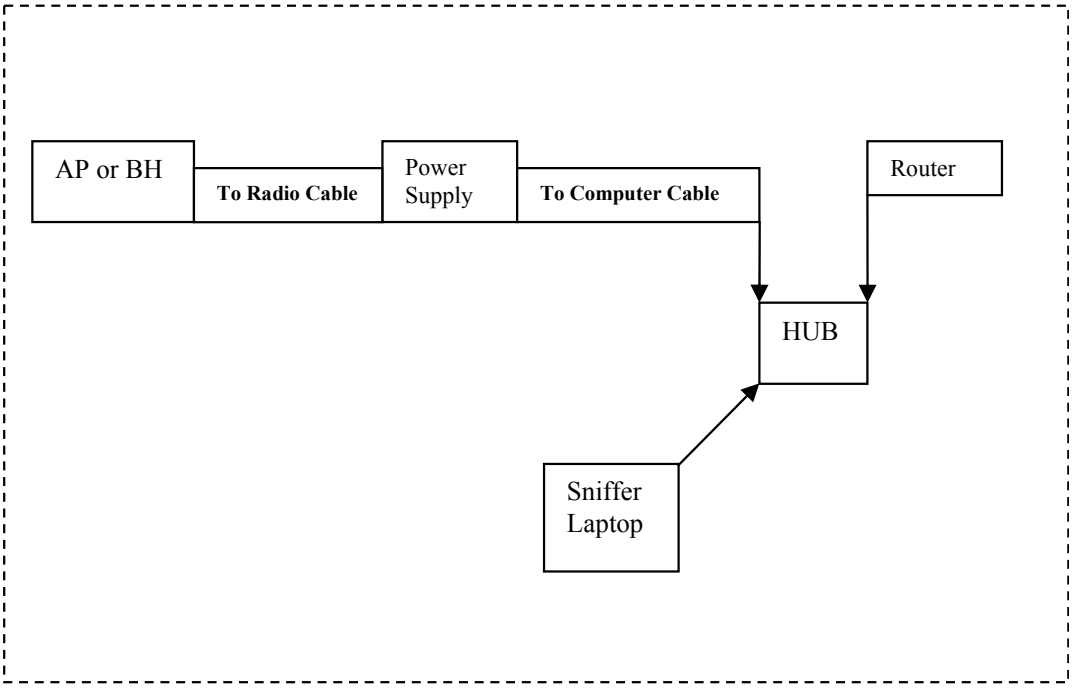


Figure 135: Protocol analysis at AP or BH not connected to a CMM

30.3 ANALYZING TRAFFIC AT AN AP OR BH WITH A CMM

The IP address of the protocol analyzer laptop computer must match the IP addressing scheme of the AP/BH. If the router is configured to be a DHCP server, then configure the laptop computer to automatically obtain an address. If DHCP is not enabled, ensure that the laptop computer is configured with a static IP address in the same subnet as the AP/BH.

Connect the hub to the J2 Ethernet to Switch of the port that is associated with the AP/BH. This example is of capturing traffic from AP/BH 111, which is connected to Port 1. The configuration for analyzing traffic at an AP or BH that is connected to a CMM is shown in Figure 136.

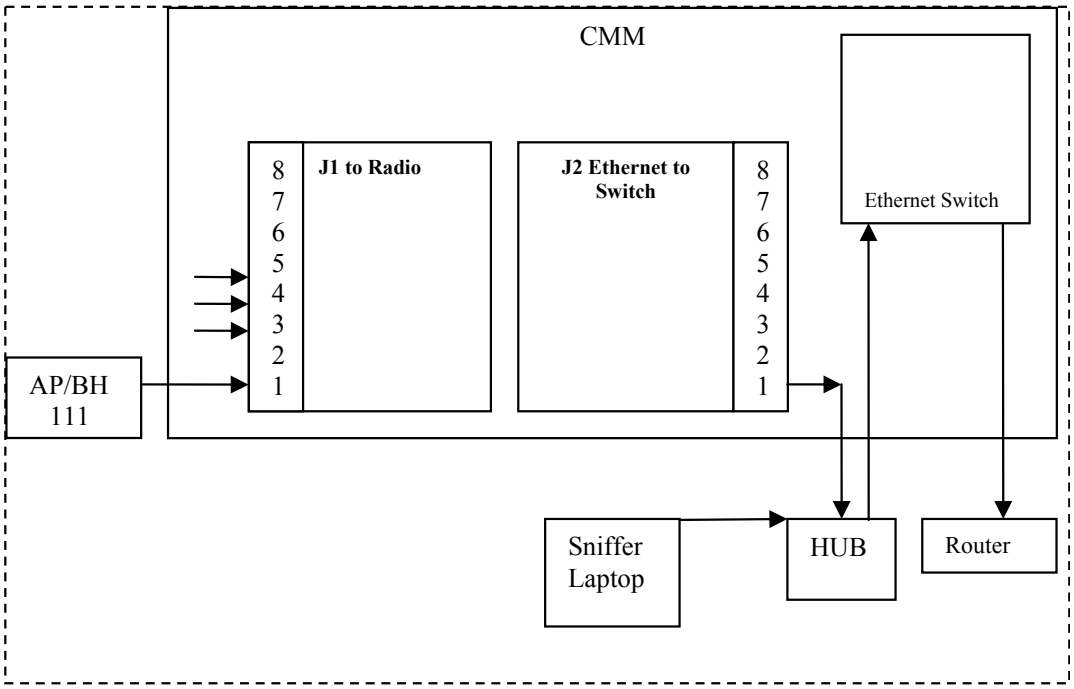


Figure 136: Protocol analysis at AP or BH connected to a CMM

30.4 EXAMPLE OF A PROTOCOL ANALYZER SETUP FOR AN SM

The following is an example of a protocol analyzer setup using Ethereal software to capture traffic at the SM level. This example is based on the following assumptions:

- All required physical cabling has been completed.
- The hub, protocol analyzer laptop computer, subscriber PC are successfully connected.
- The SM is connected
  - as shown in Figure 135 on Page 363.
  - to the subscriber PC and the AP.
- Ethereal software is operational on the laptop computer.

Although these procedures involve the SM, the only difference in the procedure for analyzing traffic on an AP or BH is the hub insertion point.

An IP configuration screen of the example SM is shown in Figure 137.

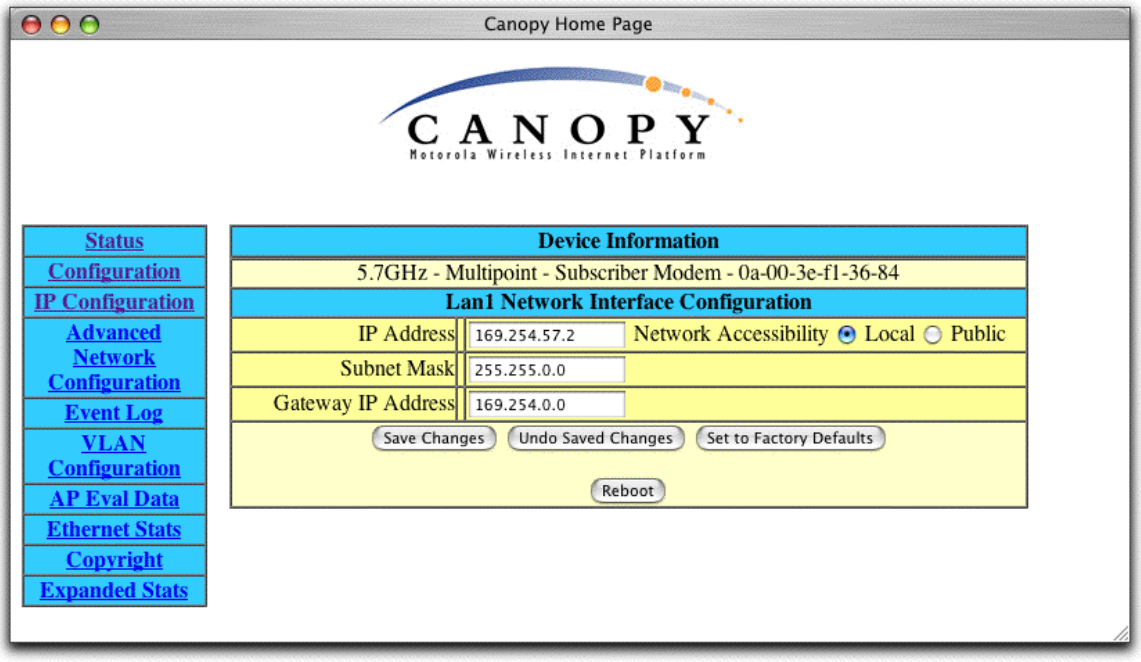


Figure 137: IP Configuration screen for SM

Verify that the current method of IP addressing is configured on the protocol analyzer laptop computer (network card). First, note the IP Configuration of the SM.

Then browse to
Start→My Network Places→Network and Dialup Connections.
For **Local Area Connection**, select **Properties**, as shown in Figure 138.

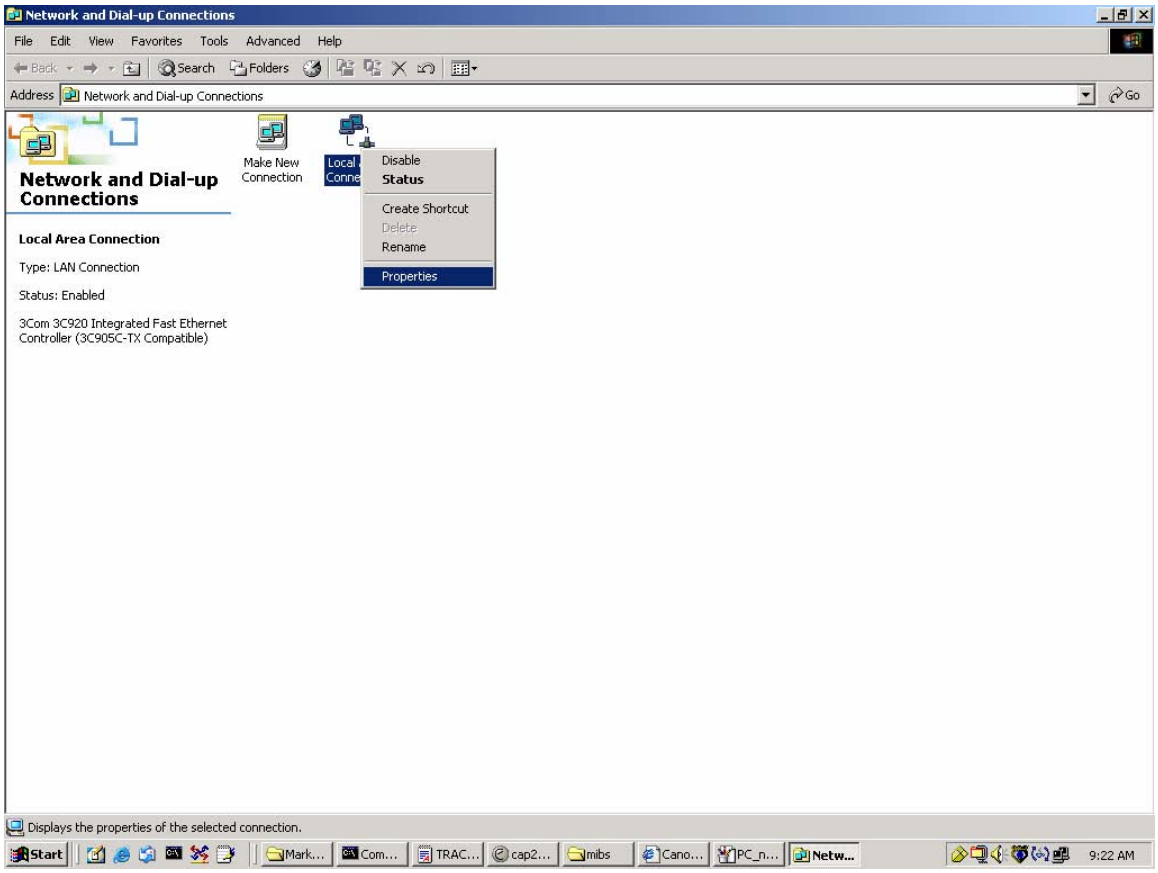


Figure 138: Local Area Connection menu

Select **Internet Protocol (TCP/IP)** as shown in Figure 139. Then click **Properties**.

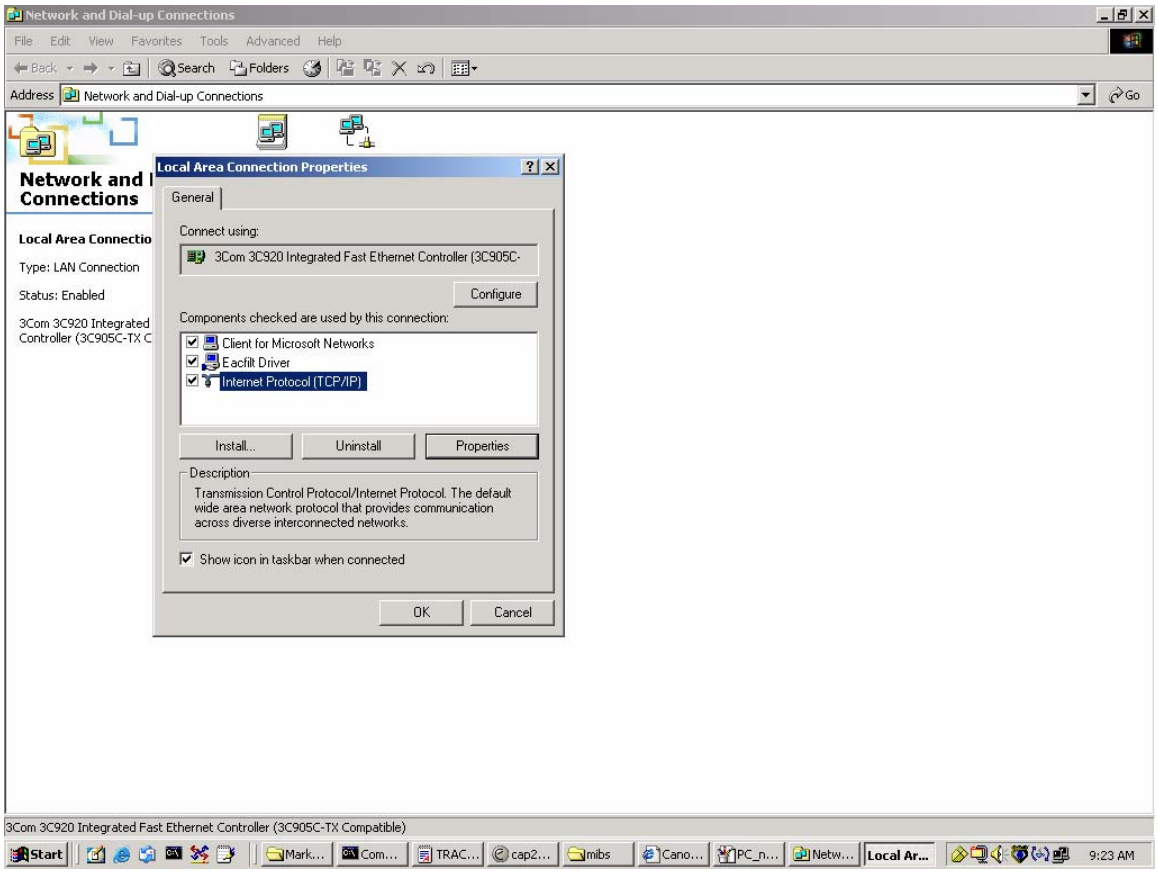


Figure 139: Local Area Connection Properties window

Unless you have a static IP address configured on the SM, select **Obtain an IP address automatically** for the protocol analyzer laptop computer, as shown in Figure 140. If you have configured a static IP address on the SM, select **Use the following IP address** and enter an IP address that is in the same subnet as the SM. Click **OK**.

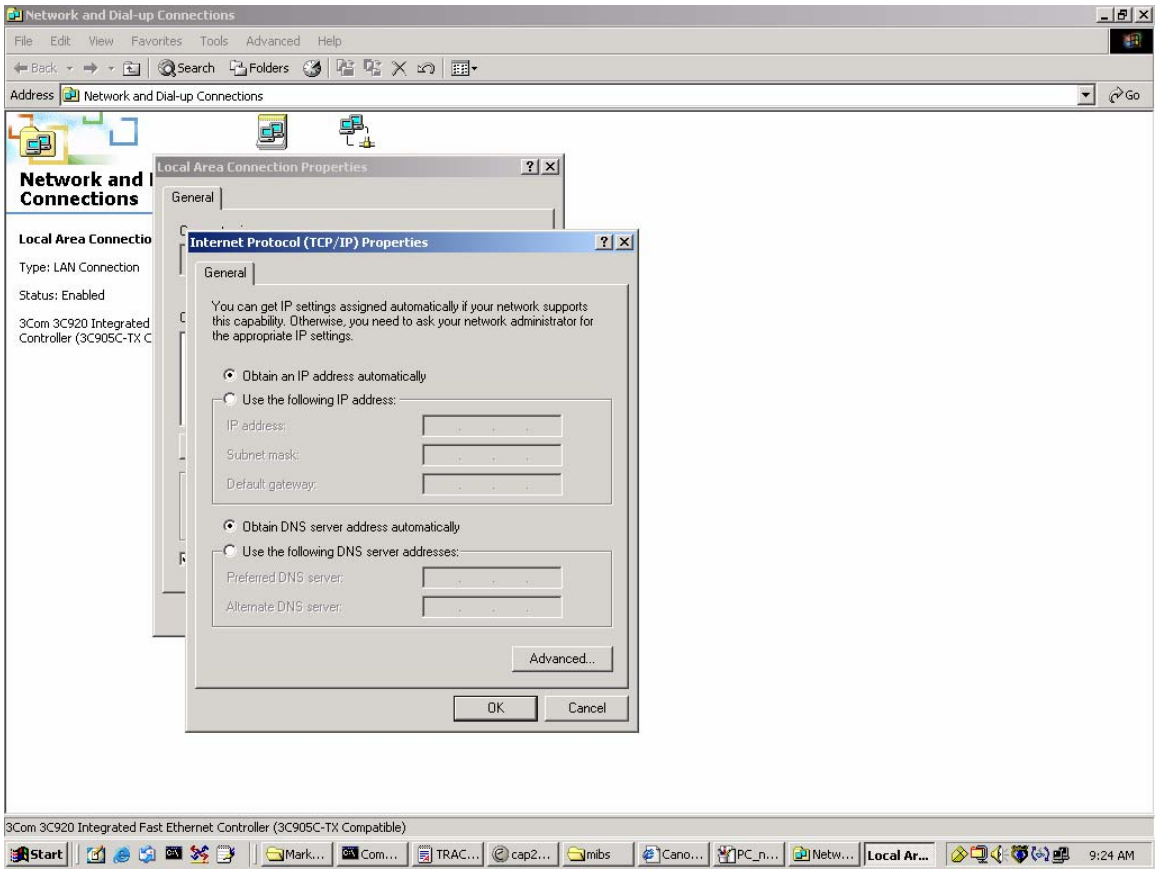

Network and Dial-up Connections
File Edit View Favorites Tools Advanced Help
Back Search Folders
Address Network and Dial-up Connections
Go
Network and Connections
Local Area Connection Properties
General
Local Area Connectio
Type: LAN Connection
Status: Enabled
3Com 3C920 Integrated Controller (3C905C-TX C
Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel
3Com 3C920 Integrated Fast Ethernet Controller (3C905C-TX Compatible)
Start
Mark... Com... TRAC... cap2... mibs Cano... PC_n... Netw... Local Ar...
9:24 AM

Figure 140: Internet Protocol (TCP/IP) Properties window

Open your Web browser and enter the address of the SM.

The Status page of the SM opens, as shown in Figure 141. If this page does not open, reconfigure how the laptop computer obtains an IP address.

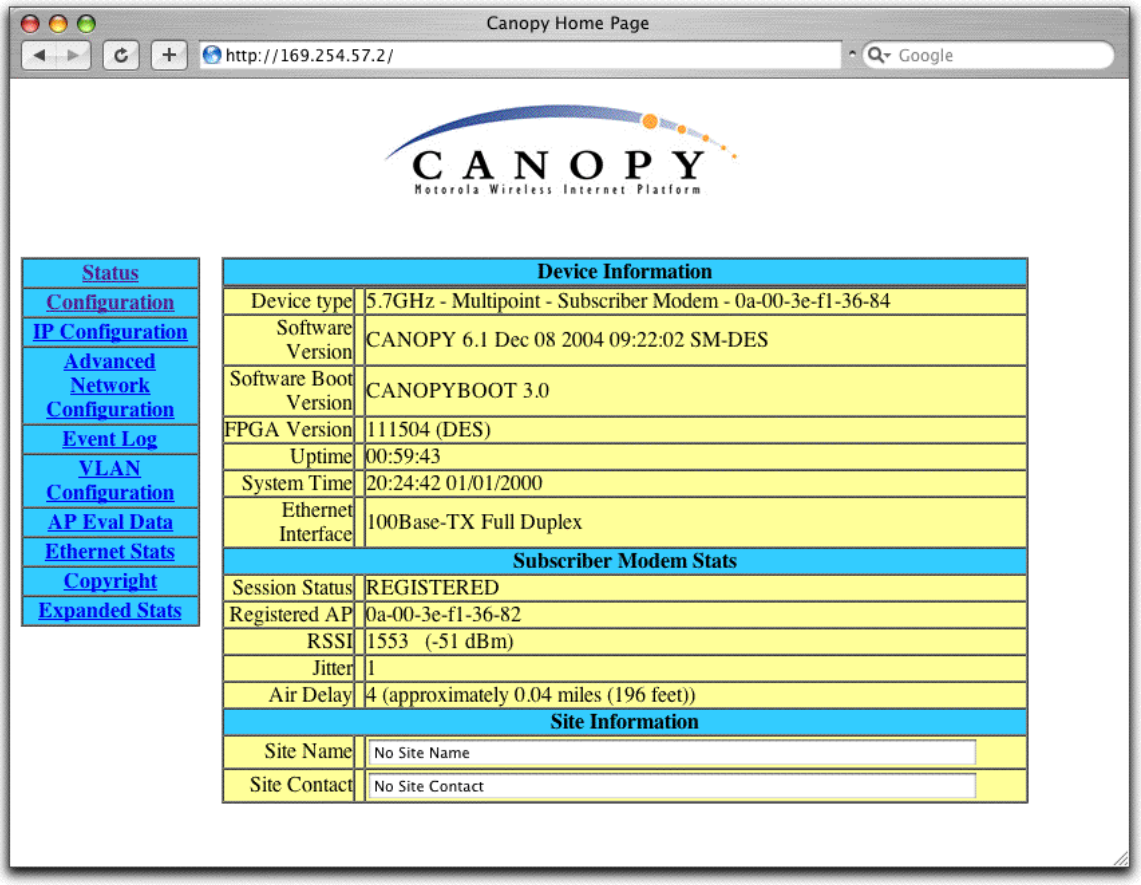


Figure 141: Status screen for SM

After you have successfully verified that you have connectivity from the laptop computer to the SM with the hub inserted, launch the protocol analyzer software on the laptop computer.

Ethereal software opens as shown in Figure 142.

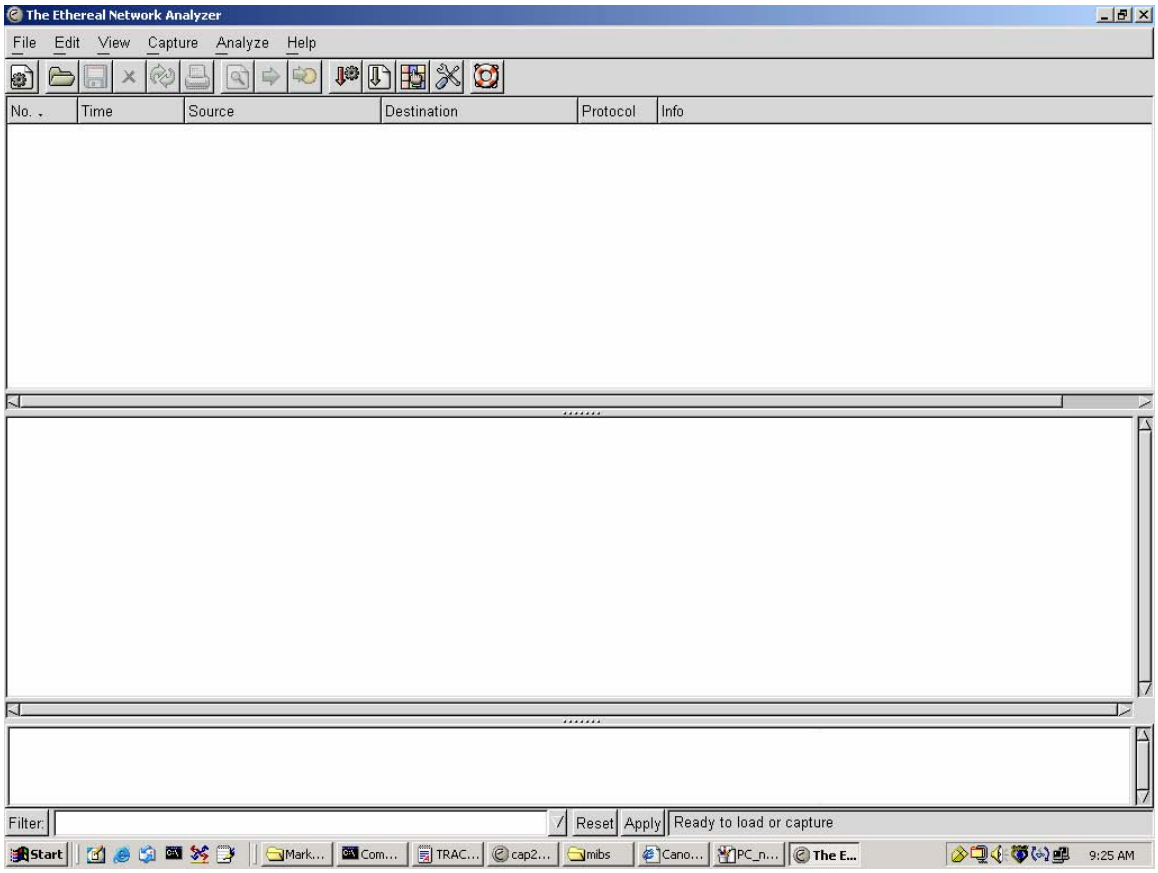


Figure 142: Ethereal software launch window

In the **Capture** menu (shown in Figure 143), select **Start**.

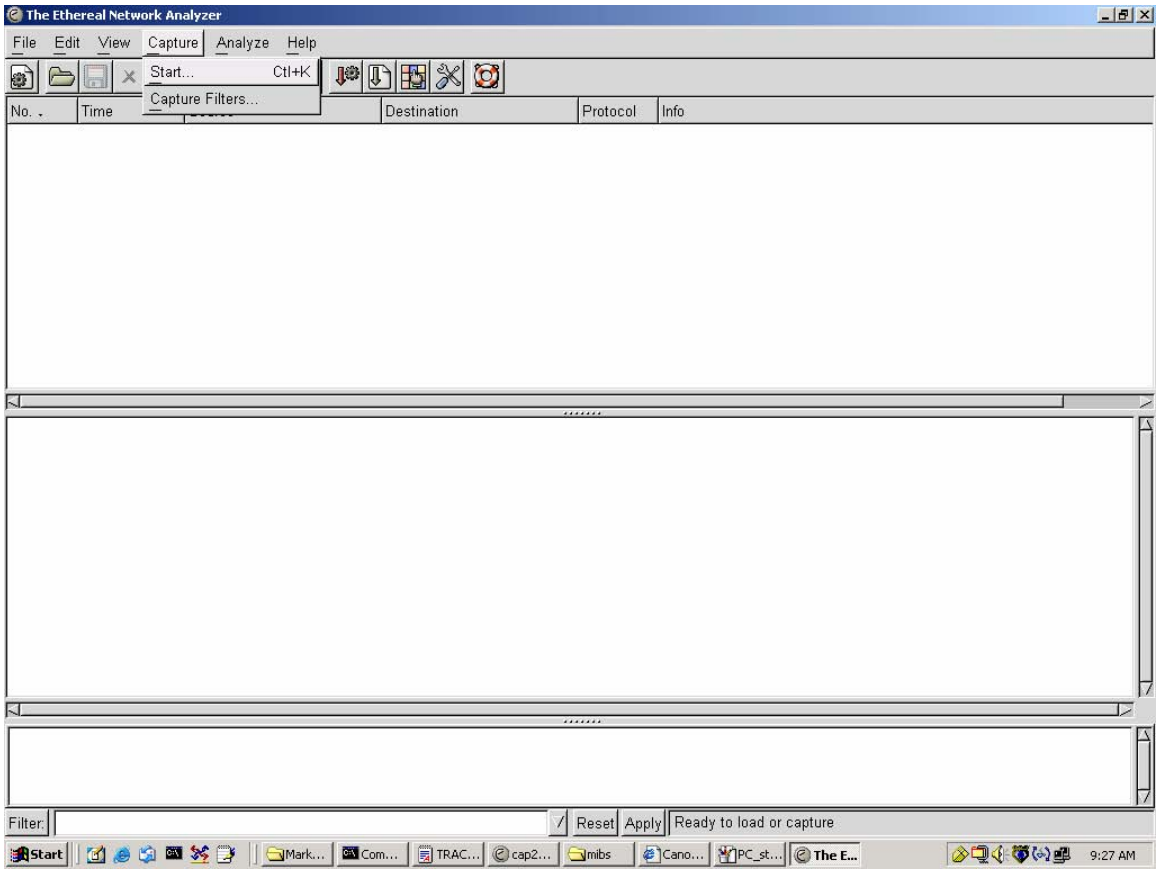


Figure 143: Capture menu

The **Ethereal Capture Options** window opens, as shown in Figure 144. Ensure that the interface reflects the network interface card (NIC) that is used on the protocol analyzer laptop computer. Although you can select filters based on specific types of traffic, all values are defaults in this example. Select filters if desired, then click **OK**.

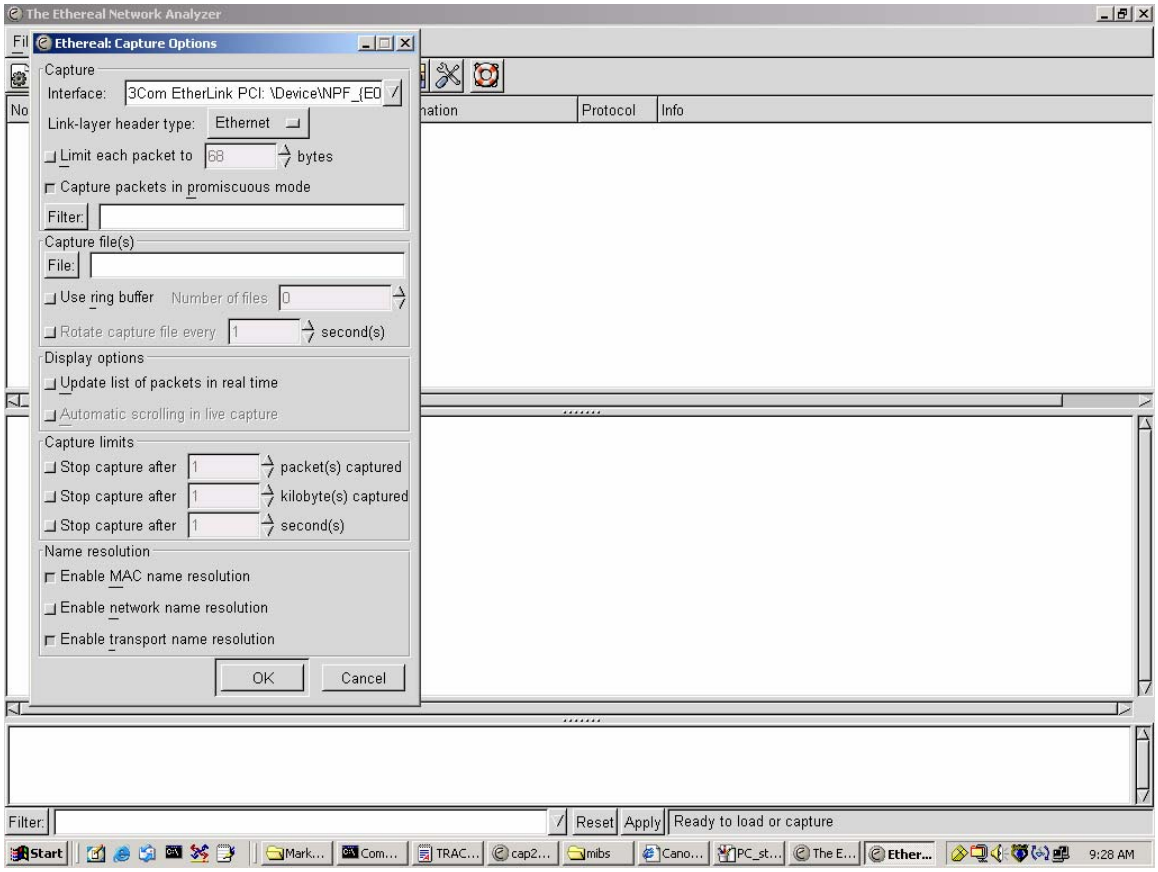


Figure 144: Ethereal Capture Options window

The **Ethereal Capture** window opens, as shown in Figure 145. This window graphically displays the types of packets (by percentage) that are being captured. If all packet types are displayed with 0%, either

- launch your Web browser on the subscriber PC for the IP address of the SM
- ping the SM from the home PC.

If still all packet types are displayed with 0%, don't see any traffic being captured, reconfigure IP addressing until you can successfully see traffic captured on the laptop computer. Whenever the desired number of packets have been captured, click **Stop**.

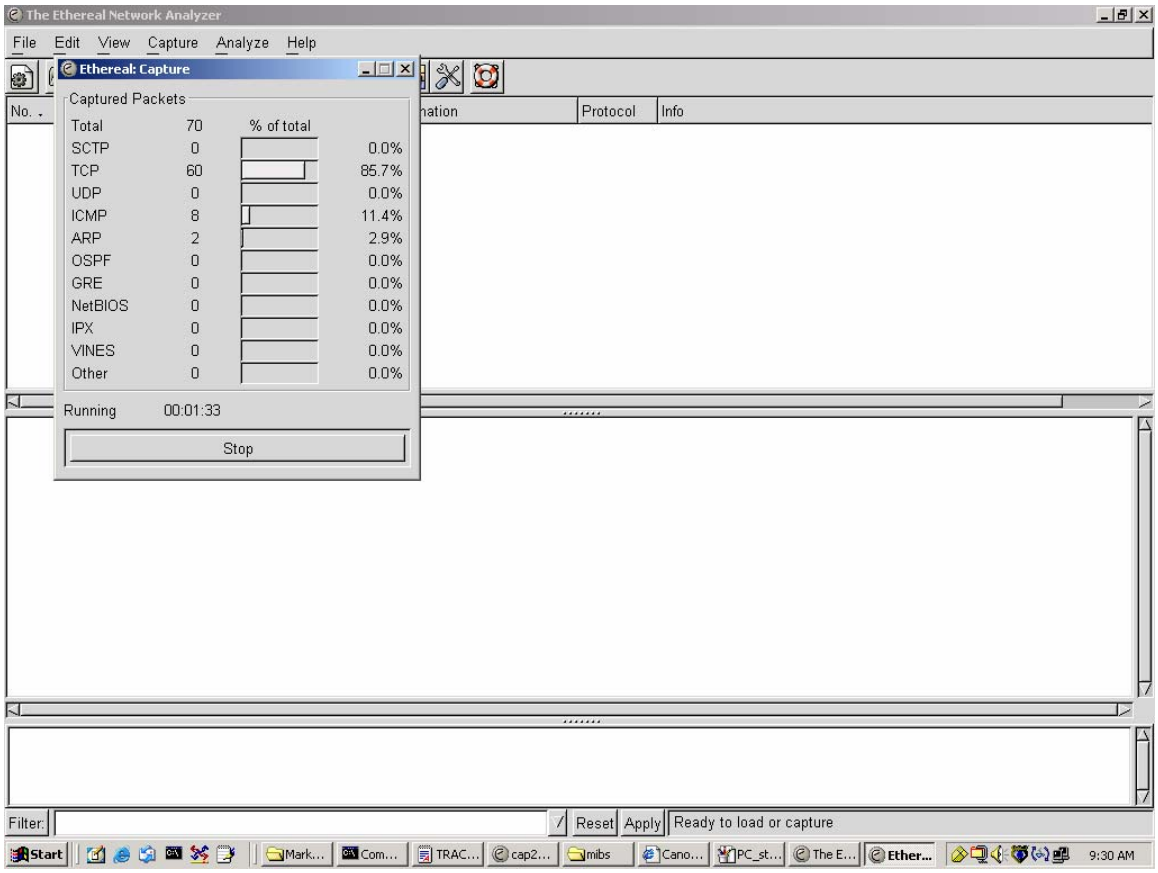


Figure 145: Ethereal Capture window

When you stop the packet capture, the **<capture> - Ethereal** window opens, as shown in Figure 146. This window has three panes:

- The top pane provides a sequenced summary of the packets captured and includes SRC/DEST address and type of protocol. What you select in this pane determines the additional information that is displayed in the lower two panes.
- The lower two panes facilitate drill-down into the packet that you selected in the top pane.

In this example, Packet 1 (a broadcast ARP request) was selected in the top pane. The lower two panes provide further details about Packet 1.

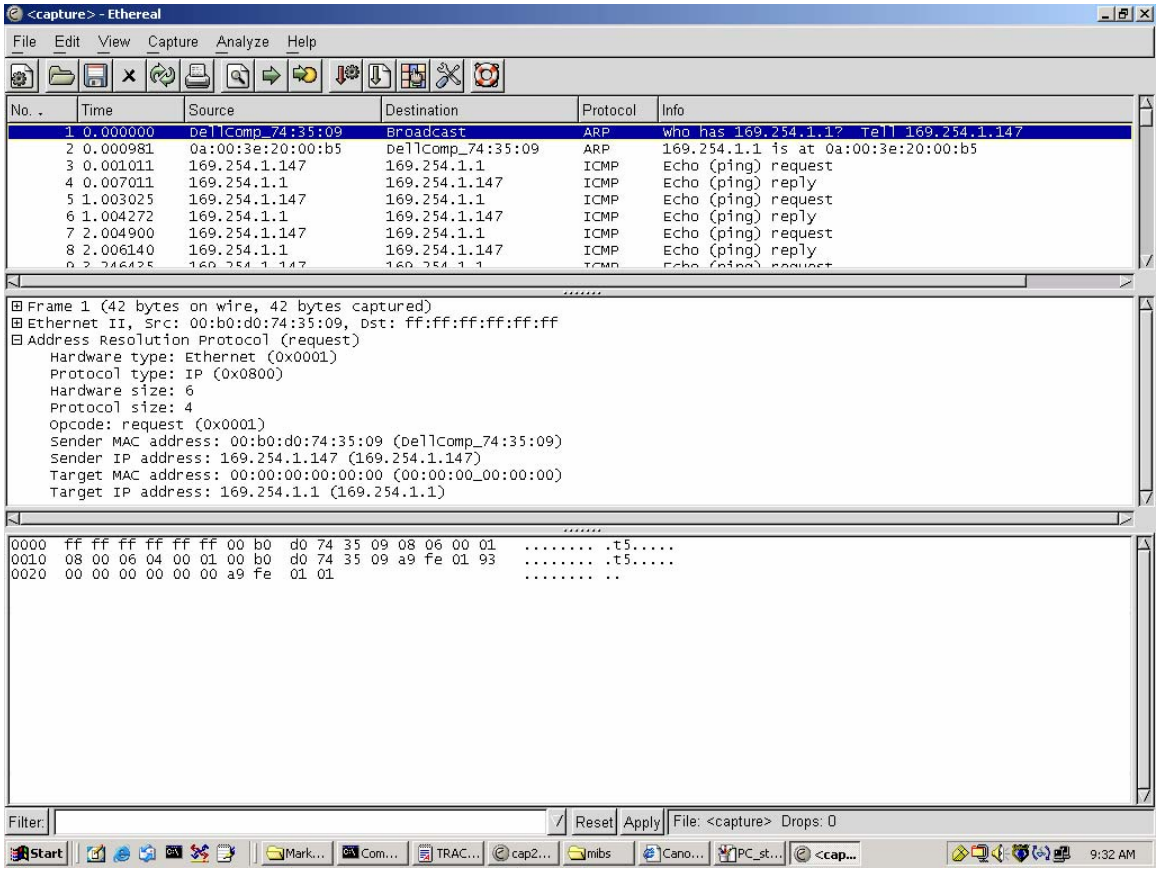

<capture> - Ethereal
File Edit View Capture Analyze Help
No. Time Source Destination Protocol Info
1 0.000000 DellComp_74:35:09 Broadcast ARP Who has 169.254.1.1? Tell 169.254.1.147
2 0.000981 0a:00:3e:20:00:b5 DellComp_74:35:09 ARP 169.254.1.1 is at 0a:00:3e:20:00:b5
3 0.001011 169.254.1.147 169.254.1.1 ICMP Echo (ping) request
4 0.007011 169.254.1.1 169.254.1.147 ICMP Echo (ping) reply
5 1.003025 169.254.1.147 169.254.1.1 ICMP Echo (ping) request
6 1.004272 169.254.1.1 169.254.1.147 ICMP Echo (ping) reply
7 2.004900 169.254.1.147 169.254.1.1 ICMP Echo (ping) request
8 2.006140 169.254.1.1 169.254.1.147 ICMP Echo (ping) reply
Frame 1 (42 bytes on wire, 42 bytes captured)
Ethernet II, Src: 00:b0:d0:74:35:09, Dst: ff:ff:ff:ff:ff:ff
Address Resolution Protocol (request)
Hardware type: Ethernet (0x0001)
Protocol type: IP (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: request (0x0001)
Sender MAC address: 00:b0:d0:74:35:09 (DellComp_74:35:09)
Sender IP address: 169.254.1.147 (169.254.1.147)
Target MAC address: 00:00:00:00:00:00 (00:00:00_00:00:00)
Target IP address: 169.254.1.1 (169.254.1.1)
0000 ff ff ff ff ff ff 00 b0 d0 74 35 09 08 06 00 01 ..... .t5.....
0010 08 00 06 04 00 01 00 b0 d0 74 35 09 a9 fe 01 93 ..... .t5.....
0020 00 00 00 00 00 00 a9 fe 01 01 ....
Filter: Reset Apply File: <capture> Drops: 0
Start
9:32 AM

Figure 146: <capture> - Ethereal window, Packet 1 selected

In the next example, Packet 14 (protocol type HTTP) is selected in the top pane, as shown in Figure 147. The two lower panes provide further details about Packet 14.

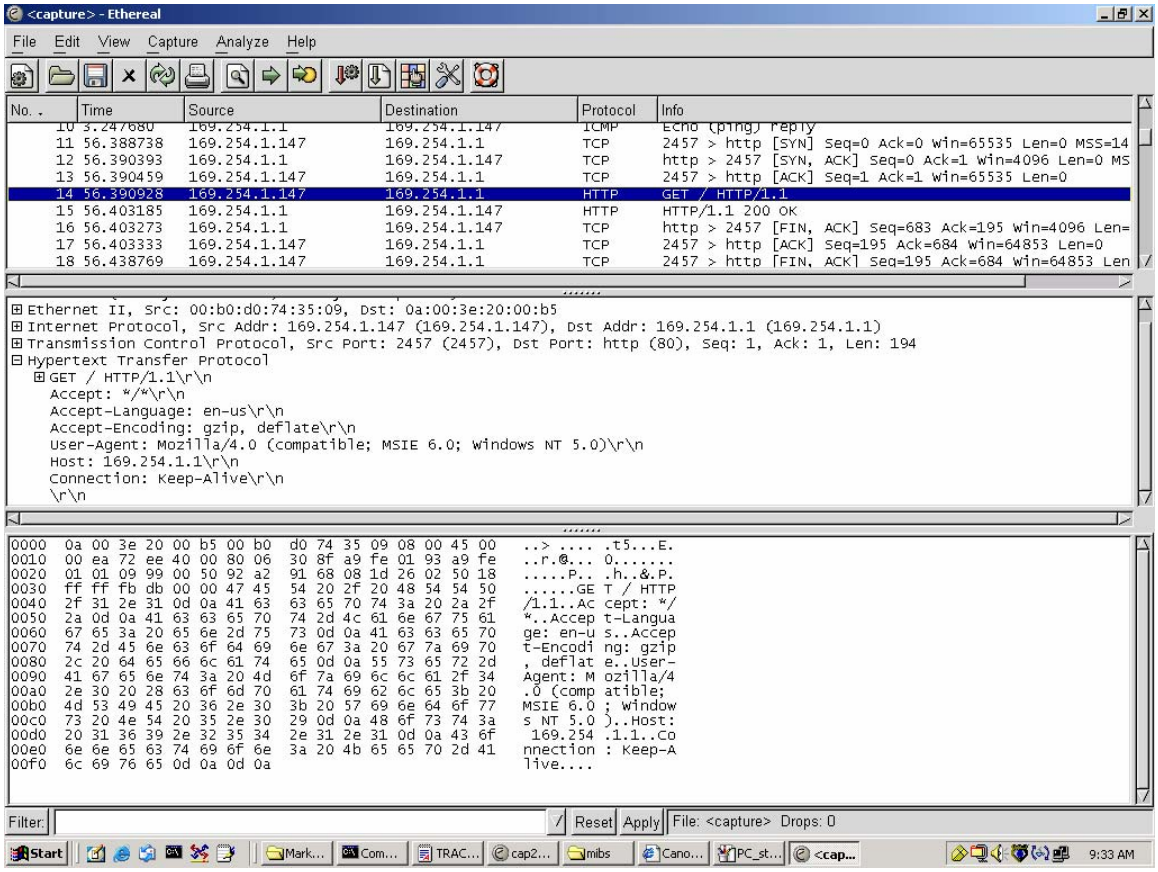


Figure 147: <capture> - Ethereal window, Packet 14 selected

31 TROUBLESHOOTING

31.1 GENERAL PLANNING FOR TROUBLESHOOTING

Effective troubleshooting depends in part on measures that you take before you experience trouble in your network. Canopy recommends the following measures for each site:

1. Identify troubleshooting tools that are available at your site (such as a protocol analyzer).
2. Identify commands and other sources that can capture baseline data for the site. These may include
   - **`ping`**
   - **`tracert`** or **`traceroute`**
   - Link Test results
   - throughput data
   - Configuration screen captures
   - Status page captures
   - session logs
3. Start a log for the site.
4. Include the following information in the log:
   - operating procedures
   - site-specific configuration records
   - network topology
   - software releases, boot versions, and FPGA firmware versions
   - types of hardware deployed
   - site-specific troubleshooting processes
   - escalation procedures
5. Capture baseline data into the log from the sources listed in Step 2.

31.2 GENERAL FAULT ISOLATION PROCESS

Effective troubleshooting also requires an effective fault isolation methodology that includes

- attempting to isolate the problem to the level of a system, subsystem, or link, such as
  - AP to SM
  - AP to CMM
  - AP to GPS
  - CMM to GPS
  - BHM to BHS

  - BHM to CMM
  - power
- researching Event Logs of the involved equipment. (See Interpreting Messages in the Event Log Page on Page 330.)
- answering the questions listed in the following section.
- reversing the last previous corrective attempt before proceeding to the next.
- performing only one corrective attempt at a time.

31.3 QUESTIONS TO HELP ISOLATE THE PROBLEM

When a problem occurs, attempt to answer the following questions:

1. What is the history of the problem?
   - Have we changed something recently?
   - Have we seen other symptoms before this?
2. How wide-spread is the symptom?
   - Is the problem on only a single SM? (If so, focus on that SM.)
   - Is the problem on multiple SMs? If so
     - is the problem on one AP in the cluster? (If so, focus on that AP)
     - is the problem on multiple, but not all, APs in the cluster? (If so, focus on those APs)
     - is the problem on all APs in the cluster? (If so, focus on the CMM and the GPS signal.)
3. Based on data in the Event Log (described in Interpreting Messages in the Event Log Page on Page 330)
   - does the problem correlate to External Hard Resets with no WatchDog timers? (If so, this indicates a loss of power. Correct your power problem.)
   - is intermittent connectivity indicated? (If so, verify your configuration, RSSI, jitter, cables and connections, and the speed duplex of both ends of the link).
   - does the problem correlate to loss-of-sync events?
4. Are connections made via *shielded* cables?
5. Does the GPS antenna have an *unobstructed* view of the entire horizon?

31.4 SECONDARY STEPS

After preliminary fault isolation through the above steps

1. check the Canopy knowledge base to find whether other network operators have encountered a similar problem.
2. proceed to any appropriate set of diagnostic steps. These are organized as follows:
   - Module Has Lost or Does Not Establish Connectivity
   - NAT/DHCP-configured SM Has Lost or Does Not Establish Connectivity on Page 379
   - SM Does Not Register to an AP on Page 380
   - BHS Does Not Register to a BHM on Page 381

◦ Module Has Lost or Does Not Gain Sync on Page 381
◦ Module Does Not Establish Ethernet Connectivity on Page 382
◦ Module Does Not Power Up on Page 382
◦ Power Supply Does Not Produce Power on Page 383
◦ CMM2 Does Not Power Up on Page 384
◦ CMM2 Does Not Pass Proper GPS Sync to Connected Modules on Page 384

31.5 PROCEDURES FOR TROUBLESHOOTING

31.5.1 Module Has Lost or Does Not Establish Connectivity

To troubleshoot a loss of connectivity, perform the following steps.

Procedure 48: Troubleshooting loss of connectivity

1. Isolate the end user/SM from peripheral equipment and variables such as routers, switches, and firewalls.
2. Set up the minimal amount of equipment.
3. On each end of the link
   a. check the cables and connections.
   b. verify that the cable/connection scheme—straight-through or crossover—is correct.
   c. verify that the LED labeled LNK is green.
   d. access the Status page of the module
   e. verify that the SM is registered.
   f. verify that RSSI is 700 or higher.
   g. verify that jitter is reported as 9 or lower.
   h. access the IP Configuration page of the module.
   i. verify that IP addresses match and are in the same subnet.
4. On the SM end of the link
   a. verify that the PC that is connected to the SM is correctly configured to obtain an IP address through DHCP.
   b. execute **`ipconfig`**.
   c. verify that the PC has an assigned IP address.
5. On each end of the link
   a. access the Configuration page of the module.
   b. verify that the settings for link negotiation, frequency, and color code match those of the other module.
   c. access the browser LAN settings (for example, at **Tools→Internet Options→Connections→LAN Settings** in Internet Explorer).
   d. verify that none of the settings are selected.
   e. access the Link Test page of the module.
   f. perform a link test.

g. verify that the link test results show efficiency greater than 90% in both the uplink and downlink.
h. execute **`ping`**.
i. verify that no packet loss was experienced.
j. verify that response times are not significantly greater than
   - 2.5 ms from BH to BH
   - 4 ms from AP to SM
   - 15 ms from SM to AP
k. replace any cables that you suspect may be causing the problem.

6. After connectivity has been re-established, reinstall network elements and variables that you removed in Step 1.

end of procedure

31.5.2 NAT/DHCP-configured SM Has Lost or Does Not Establish Connectivity

Before troubleshooting this problem, identify the NAT/DHCP configuration from the following list:

- NAT with DHCP Client and DHCP Server
- NAT with DHCP Client
- NAT with DHCP Server
- NAT without DHCP

To troubleshoot a loss of connectivity for an SM configured for NAT/DHCP, perform the following steps.

Procedure 49: Troubleshooting loss of connectivity for NAT/DHCP-configured SM

1. Isolate the end user/SM from peripheral equipment and variables such as routers, switches, and firewalls.
2. Set up the minimal amount of equipment.
3. On each end of the link
   a. check the cables and connections.
   b. verify that the cable/connection scheme—straight-through or crossover—is correct.
   c. verify that the LED labeled LNK is green.
4. At the SM
   a. select Expanded Stats.
   b. access the NAT Table page.
   c. verify that the correct NAT translations are listed.
      RESULT: NAT is eliminated as a possible cause if these translations are correct.
5. If this SM is configured for NAT with DHCP, then at the SM
   a. execute **ipconfig**.
   b. verify that the PC has an assigned IP address.

c. if the PC *does not* have an assigned IP address, then
   - enter **`ipconfig /release "Adapter Name"`**.
   - enter **`ipconfig /renew "Adapter Name"`**.
   - reboot the PC.
   - retreat to Step 5a.

d. if the PC has an assigned IP address, then
   - access the DHCP pages of the SM.
   - verify that DHCP is operating as configured.

6. After connectivity has been re-established, reinstall network elements and variables that you removed in Step 1.

end of procedure

31.5.3 SM Does Not Register to an AP

To troubleshoot an SM failing to register to an AP, perform the following steps.

Procedure 50: Troubleshooting SM failing to register to an AP

1. Access the Configuration page of the SM.
2. Note the **Color Code** of the SM.
3. Access the Configuration page of the AP.
4. Verify that the **Color Code** of the AP matches that of the SM.
5. Note the **RF Frequency Carrier** of the AP.
6. Verify that the value of the **RF Frequency Carrier** of the AP is selected in the **Custom RF Frequency Scan Selection List** parameter on the Configuration page of the SM.
7. On the Configuration page of the AP, verify that the **Max Range** parameter is set to a distance slightly greater than the distance between the AP and the furthest SM that must register to this AP.
8. Verify that a clear line of sight exists between the AP and the SM, and that no obstruction significantly penetrates the Fresnel zone of the attempted link. If these conditions are not established, then verify that the AP and SM are 900-MHz modules in close proximity to each other.
9. Verify that both the AP and SM are of the same frequency band range and encryption (for example, 5200AP and 5200SM).
10. Remove the bottom cover of the SM to expose the LEDs.
11. Power cycle the SM.
    RESULT: Approximately 25 seconds after the power cycle, the green LED labeled LNK should light to indicate that the link has been established. If the orange LED labeled SYN is lit instead, then the SM is in Alignment mode because the SM failed to establish the link.
12. In this latter case, and if the SM has encountered no customer-inflicted damage, then request an RMA for the SM.

end of procedure

31.5.4 BHS Does Not Register to a BHM

To troubleshoot an BHS failing to register to a BHM, perform the following steps.

Procedure 51: Troubleshooting BHS failing to register to a BHM

1. Access the Configuration page of the BHS.
2. Note the **Color Code** of the BHS.
3. Access the Configuration page of the BHM.
4. Verify that the **Color Code** of the BHM matches that of the BHS.
5. Note the **RF Frequency Carrier** of the BHM.
6. Verify that the value of the **RF Frequency Carrier** of the BHM is selected in the **Custom RF Frequency Scan Selection List** parameter on the Configuration page of the BHS.
7. Verify that a clear line of sight exists between the AP and the SM, and that no obstruction significantly penetrates the Fresnel zone of the attempted link.
8. Verify that both the BHM and BHS are of the same frequency band range and encryption (for example, 5200BH and 5200BH).
9. Remove the bottom cover of the BHS to expose the LEDs.
10. Power cycle the SM.
    RESULT: Approximately 25 seconds after the power cycle, the green LED labeled LNK should light to indicate that the link has been established. If the orange LED labeled SYN is lit instead, then the SM is in Alignment mode because the SM failed to establish the link. In this latter case, and if the SM has encountered no customer-inflicted damage, then request an RMA for the SM.

========== **end of procedure** ==========

31.5.5 Module Has Lost or Does Not Gain Sync

To troubleshoot a loss of sync, perform the following steps.

Procedure 52: Troubleshooting loss of sync

1. Access the Event Log page of the SM.
2. Check for messages with the following format:
   `RcvFrmNum =`
   `ExpFrmNum =`
   (See Table 60: Event Log messages for abnormal events on Page 332.)
3. If these messages are present, check the Event Log page of another SM that is registered to the same AP for messages of the same type.
4. If the Event Log of this second SM *does not* contain these messages, then the fault is isolated to the first SM.
5. If the Event Log page of this second SM contains these messages, access the GPS Status page of the AP.
6. If the **Satellites Tracked** field in the GPS Status page of the AP indicates fewer than 4 or the **Pulse Status** field does not indicate Generating Sync, check the GPS Status page of another AP in the same AP cluster for these indicators.

7. If these indicators are present in the second AP
   a. verify that the GPS antenna still has an unobstructed view of the entire horizon.
   b. visually inspect the cable and connections between the GPS antenna and the CMM.
   c. if this cable is not shielded, replace the cable with shielded cable.
8. If these indicators *are not* present in the second AP
   a. visually inspect the cable and connections between the CMM and the AP antenna.
   b. if this cable is not shielded, replace the cable with shielded cable.

========== **end of procedure** ==========

31.5.6 Module Does Not Establish Ethernet Connectivity

To troubleshoot a loss of Ethernet connectivity, perform the following steps.

Procedure 53: Troubleshooting loss of Ethernet connectivity

1. Verify that the connector crimps on the Ethernet cable are not loose.
2. Verify that the Ethernet cable is not damaged.
3. If the Ethernet cable connects the module to a network interface card (NIC), verify that the cable is pinned out as a straight-through cable.
4. If the Ethernet cable connects the module to a hub, switch, or router, verify that the cable is pinned out as a crossover cable.
5. Verify that the Ethernet port to which the cable connects the module is set to auto-negotiate speed.
6. Power cycle the module.
7. ***RESULT:*** Approximately 25 seconds after the power cycle, the green LED labeled LNK should light to indicate that the link has been established. If the orange LED labeled SYN is lit instead, then the module is in Alignment mode because the module failed to establish the link.
8. In this latter case, and if the module has encountered no customer-inflicted damage, then request an RMA for the module.

========== **end of procedure** ==========

31.5.7 Module Does Not Power Up

To troubleshoot the failure of a module to power up, perform the following steps.

Procedure 54: Troubleshooting failure to power up

1. Verify that the connector crimps on the Ethernet cable are not loose.
2. Verify that the Ethernet cable is not damaged.
3. Verify that the cable is wired and pinned out according to the specifications provided under Wiring Connectors on Page 137.

4. Remove the cover of the module to expose the components on the printed wiring board.
5. Find the Ethernet transformer, which is labeled with either the name Halo or the name Pulse.
6. Verify that the Ethernet transformer does not show damage that would have been caused by improper cabling. (You can recognize damage as the top of the transformer being no longer smooth. The transformer in the following picture is damaged and is ineligible for an RMA.)

7. Connect the power supply to a known good Canopy module via a known good Ethernet cable.
8. Attempt to power up the known good module and
   - if the known good module fails to power up, request an RMA for the power supply.
   - if the known good module powers up, return to the module that does not power up.
9. Reconnect the power supply to the failing module.
10. Connect the power supply to a power source.
11. Verify that the red LED labeled PWR lights.
12. If this LED *does not* light, and the module has not been powered up since the last previous FPGA firmware upgrade was performed on the module, the request an RMA for the module.

========== **end of procedure** ==========

31.5.8 Power Supply Does Not Produce Power

To troubleshoot the failure of a power supply to produce power, perform the following steps.

Procedure 55: Troubleshooting failure of power supply to produce power

1. Verify that the connector crimps on the Ethernet cable are not loose.
2. Verify that the Ethernet cable is not damaged.
3. Verify that the cable is wired and pinned out according to the specifications provided under Wiring Connectors on Page 137.
4. Connect the power supply to a known good Canopy module via a known good Ethernet cable.

5. Attempt to power up the known good module.
6. If the known good module fails to power up, request an RMA for the power supply.

end of procedure

31.5.9 CMM2 Does Not Power Up

To troubleshoot a malfunctioning CMM2, perform the following steps.

Procedure 56: Troubleshooting CMM2 that malfunctions

1. Verify that the 115-/230-V switch (in the lower right-hand corner of the CMM2) is in the correct position for the power source. (See Figure 101 on Page 264.) Applying power when this switch is in the wrong position can damage the CMM2 and will render it ineligible for an RMA.
2. Verify that the electrical source to the CMM2 meets Canopy specifications. See Table 14 on Page 53.
3. Verify that the electrical source is connected to the CMM2 at the proper connection point. (See Figure 103 on Page 266.)
4. Verify that the fuse is operational.
5. Verify that the fuse is properly seated in the receptacle.
6. Attempt to power up the CMM2.
7. If the power indicator on the interconnect board of the CMM2 fails to light when power is applied to the CMM2, request an RMA for the CMM2.

end of procedure

31.5.10 CMM2 Does Not Pass Proper GPS Sync to Connected Modules

If the Event Log pages of all connected modules contain `Loss of GPS Sync Pulse` messages, perform the following steps.

Procedure 57: Troubleshooting CMM2 not passing sync

1. Verify that the GPS antenna has an unobstructed view of the entire horizon.
2. Verify that the GPS coaxial cable meets specifications.
3. Verify that the GPS sync cable meets specifications for wiring and length.
4. If the web pages of connected modules indicate any of the following, then find and eliminate the source of noise that is being coupled into the GPS sync cable:
   - In the GPS Status page
     - anomalous number of **Satellites Tracked** (greater than 12, for example)
     - incorrect reported **Latitude** and/or **Longitude** of the antenna
   - In the Event Log page
     - garbled GPS messages
     - large number of `Acquired GPS Sync Pulse` messages

5. If these efforts fail to resolve the problem, then request an RMA for the CMM2.

end of procedure

31.5.11 Module Software Cannot be Upgraded

If your attempt to upgrade the software of a module fails, perform the following steps.

Procedure 58: Troubleshooting an unsuccessful software upgrade

1. Download the latest issue of the target release and the associated release notes.
2. Compare the files used in the failed attempt to the newly downloaded software.
3. Compare the procedure used in the failed attempt to the procedure in the newly downloaded release notes.
4. If these comparisons reveal a difference, retry the upgrade, this time with the newer file or newer procedure.
5. If, during attempts to upgrade the FPGA firmware, the following message is repeatable, then request an RMA for the module:

   ```
   Error code 6, unrecognized device
   ```

end of procedure

31.5.12 Module Functions Properly, Except Web Interface Became Inaccessible

If a module continues to pass traffic, and the telnet and SNMP interfaces to the module continue to function, but the web interface to the module does not display, perform the following steps.

Procedure 59: Restoring the web interface to a module

1. Enter **`telnet`** ***`DottedIPAddress`***.
   RESULT: A telnet session to the module is invoked.
2. At the `Login` prompt, enter **`root`**.
3. At the `Password` prompt, enter ***`PasswordIfConfigured`***.
4. At the `Telnet +>` prompt, enter **`reset`**.
   RESULT: The web interface is accessible again, and this telnet connection is closed.

end of procedure

32 OBTAINING TECHNICAL SUPPORT

NOTE:
The contact information for Canopy Technical Support staff is included at the end of this section (on Page 390). However, in most cases, you should follow the procedure of this section before you contact them.

To get information or assistance as soon as possible for problems that you encounter, use the following sequence of actions:

1. Search this document, the user guides of products that are supported by dedicated documents, and the software release notes of supported releases
   a. in the Table of Contents for the topic.
   b. in the Adobe Reader® search capability for keywords that apply.[17]
2. Visit http://www.canopywireless.com/kbase to view the Canopy Knowledge Base.
3. Ask your Canopy products supplier to help.
4. View and analyze event logs, error messages, and debug messages to help isolate the problem.
5. Check release notes and verify that all of your Canopy equipment is on the correct software release.
6. Verify that the Canopy configuration files match the last known good (baseline) Canopy configuration files captured in the site log book.
7. Verify connectivity (physical cabling).
8. At the SM level, minimize your network configuration (remove home network devices to help isolate problem).
9. Perform the site verification checklist.
10. Use Table 62 (two pages) as a job aid to collect basic site information for technical support to use.

[17] Reader is a registered trademark of Adobe Systems, Incorporated.

Table 62: Basic site information for technical support

Call Log Number:	Company:	Location:
Problem Type:	Site Contact:	Site Phone:
Call Severity (Select One): 1- Urgent-Customer Svc Down 2- Serious- Customer Svc Impacted 3- Non-Critical/General Inquiry	Open Date:	Close Date:
Product Types Involved: (ID the product type) 2400 SM/AP/BHM/BHS 5200 ER /BHM/BHS 5200 SM/AP/BHM/BHS 5700 SM/AP/BHM/BHS 1008CK 300SS ACPS110	MAC Addresses:	IP Addresses:
Software Releases:	Boot Versions:	FPGA Versions:
Authentication ?: Yes/No Type:	Is the customer using shielded cables? Yes/No	Remote Access Method: IP Address:

Network Scenario for this issue: (ID those that apply) SM to Subscriber PC Yes/No SM to AP (Point to Multipoint) Yes/No BHM to BHS (Point to Point) Yes/No 20Meg or 10Meg backhaul Yes/No	Link Distance: dBm= Jitter=	Reflectors in use: Yes/No
NAT/DHCP Scenario: NAT Disabled Yes/No NAT with DHCP Client and DHCP Server Yes/No NAT with DHCP Client Yes/No NAT with DHCP Server Yes/No NAT with no DHCP Yes/No	Problem Description: New Install: Yes/No	NAT/DHCP Scenario: NAT Disabled Yes/No NAT with DHCP Client and DHCP Server Yes/No NAT with DHCP Client Yes/No NAT with DHCP Server Yes/No NAT with no DHCP Yes/No

11. Save your basic site information as file `Site_Info`.
12. From among Figure 34 on Page 79, Figure 35 on Page 80, and Figure 36 on Page 80, select the basic network topology diagram that most closely matches your network configuration.
13. If you selected Figure 34.
    a. Indicate how many APs are in each cluster.
    b. Indicate how many AP clusters are deployed (and what types).
    c. Include the IP addresses.
    d. Indicate the frequency for each sector.
    e. Indicate the type of synchronization.
    f. Indicate how much separation exists between clusters.
    g. For each AP collect the following additional information:
        - Sector number:
        - SW release:

- Frequency:
- Color code:
- IP address:
- Downlink/uplink ratio:
- Max range:
- Bridge entry timeout:
- Number of subscribers:
- Method of synchronization:

14. If you selected Figure 35
    a. Indicate how many APs are in each cluster.
    b. Indicate how many AP clusters are deployed (and what types).
    c. Indicate how many BH links are configured.
    d. Include the IP addresses.
    e. Indicate the frequency for each sector.
    f. Indicate the type of synchronization.
    g. Indicate how much separation exists between clusters and BHs.
    h. Indicate the types of BH links (10-Mbps or 20-Mbps).
    i. Distances of links.
    j. Frequency used by each BH.
    k. For each AP and BHM, collect the following additional information:
        - Sector number:
        - SW release:
        - Frequency:
        - Color code:
        - IP address:
        - Downlink/uplink ratio:
        - Max range:
        - Bridge entry timeout:
        - Number of subscribers:
        - Method of synchronization:
15. If you selected Figure 36, collect the following additional information:
    - Sector number:
    - SW release:
    - Frequency:
    - Color code:
    - IP address:
    - Downlink/uplink ratio:
    - Max range:
    - Bridge entry timeout:
    - Number of subscribers:

- Method of synchronization:

16. Add any details that are not present in the generic diagram that you selected.
17. Save your diagram as file `Net_Diagram`.
18. Capture screens from the following web pages of affected modules:
    - Status as file *`SM/AP/BHM/BHS`*`_Status.gif`
    - Configuration as file *`SM/AP/BHM/BHS`*`_Config.gif`
    - IP Configuration as file *`SM/AP/BHM/BHS`*`_IPconfig.gif`
    - Sessions as file *`SM/AP/BHM/BHS`*`_Sessions.gif`
    - Event Log as file *`SM/AP/BHM/BHS`*`_Events.gif`
    - Link Test (with link test results) as file *`SM/AP/BHM/BHS`*`_LinkTST.gif`
    - RF Stat as file *`SM/AP/BHM/BHS`*`_RFstats.gif`
19. For any affected SM or BHS, capture screens from the following additional web pages:
    - AP Eval Data as file *`SM/BHS`*`_APEval.gif`
    - SM Sync Log as file *`SM/BHS`*`_SMSync.gif`
    - SM Session Log as file *`SM/BHS`*`_SMSess.gif`
    - SM CCenter Log as file *`SM/BHS`*`_SMCcent.gif`
20. For any affected SM that has NAT/DHCP enabled, capture screens from the following additional web pages:
    - NAT Configuration as file *`SM`*` _Natconfig.gif`
    - NAT Table as file *`SM`*` _NatTable.gif`
    - NAT Stats as file *`SM`*` _NatStats.gif`
    - ARP Stats as file *`SM`*` _ArpStats.gif`
    - DHCP Stats as file *`SM`*` _DhcpStats.gif`
    - DHCP Client Log as file *`SM`*` _DhcpClient.gif`
    - DHCP Info Log as file *`SM`*` _DhcpInfo.gif`
    - DHCP Server Log as file *`SM`*` _DhcpServer.gif`

    Also capture the Windows 2000 IP Configuration screen as file *`SM`*` _WindowsIP.gif`.
21. Escalate the problem to Canopy systems Technical Support (or another technical support organization that has been designated for you) as follows:
    a. Start e-mail to technical-support@canopywireless.com. In this email
        - Describe the problem.
        - Describe the history of the problem.
        - List your attempts to solve the problem.
        - Attach the above files.
        - List the files that you are attaching.
    b. Send the email.
    c. Call 1 888 605 2552 (or +1 217 824 9742).

========== **end of procedure** ==========

33 GETTING WARRANTY ASSISTANCE

For warranty assistance, contact your reseller or distributor for the process.

CANOPY SYSTEM REFERENCE INFORMATION

34 ADMINISTERING MODULES THROUGH TELNET INTERFACE

In the telnet administrative interface to a module that operates on Canopy System Release 4.2 or later release, the Canopy platform supports the commands defined in Table 63. Many of these are not needed with CNUT.

Table 63: Supported telnet commands for module administration

Command	System help Definition	Notes
addwebfile	Add a custom web file	Syntax: **addwebfile *filename***. Copies the custom web file *filename* to non-volatile memory.
burnfile	Burn flash from file	Syntax: **burnfile *filename***. Updates the CPU firmware with a new image. User the image contained in *filename* if *filename* is provided. If provided, *filename* must match the module type (for example, SMboot.bin for a Subscriber Module or APboot.bin for an Access Point Module).
cat	Concatenate and display.	Syntax: **cat *filename***. Displays the contents of *filename*.
clearsyslog	Clear the system event log	Syntax: **clearsyslog**. Clears the system event log.
clearwebfile	Clear all custom web files	Syntax: **clearwebfile**. Deletes all *custom* web files.
exit	Exit from telnet session	Syntax: **exit**. Terminates the telnet interface session.
fpga_conf	Update FPGA program	Syntax: **fpga_conf**. Forces a module to perform a hard (FPGA and CPU) reset. (See reset.)
ftp	File transfer application	Syntax: **ftp**. Launches the ftp client application on the module.
help	Display command line function help	Syntax: **help**. Displays a list of available telnet commands and a brief description of each.
jbi	Update FPGA program	Syntax: **jbi -aprogram *file.jbc***. Updates the FPGA firmware with the new image contained in *file.jbc*.

Command	System help Definition	Notes
ls	List the contents of a directory	Syntax: **ls**. Lists the file names of all files in the directory. Syntax: **ls -l**. Displays additional information, such as the sizes and dates of the files.
lsweb	List Flash Web files	Syntax: **lsweb**. Lists the file names of the saved custom web files.
ping	Send ICMP ECHO_REQUEST packets to network hosts	Syntax: **ping *IPaddress***. Sends an ICMP ECHO_REQUEST to *IPaddress* and waits for a response. If a response is received, the system returns *IPaddress* is alive. If no response is received, the system returns no answer from *IPaddress*.
reset	Reboot the unit	Syntax: **reset**. Forces the module to perform a hard (FPGA and CPU) module reset. (See **fpga_conf**.)
rm	Remove (unlink) files	Syntax: **rm *filename***. Remove *filename*.
syslog	Display system event log: syslog <optional filename>	Syntax: **syslog**. Displays the contents of the system log. Syntax: **syslog *filename***. Saves the contents of the system log to *filename*. Caution: overwrites *filename* if it already exists.
telnet	Telnet application	Syntax: **telnet *hostIPaddress***. Launches the telnet client application on the Canopy module.
tftp	tftp application	Syntax: **tftp *hostIPaddress***. Launches the tftp client application on the Canopy module.
update	Enable automatic SM code updating	Syntax: **update *actionlist.txt***. Enables the automated update procedure that *actionlist.txt* specifies. (Supported for only the Access Point Module.)
updateoff	Disable automatic SM code updating	Syntax: **updateoff**. Disables the automated update procedure.
version	Display the software version string	Syntax: **version**. Displays the module version string, which contains the software/firmware/hardware versions, the module type, and the operating frequency.

35 MANAGING THROUGH A BAM COMMAND-LINE INTERFACE

The following sections list and describe SSE commands to interface with the MySQL or PostgreSQL database. For further information about

- BAM, see Canopy Bandwidth and Authentication Manager (BAM) User Guide at http://www.motorola.com/canopy.
- PostgreSQL databases, see the index of PostgreSQL documentation at http://www.postgresql.org/docs.
- MySQL databases, see *MySQL® Reference Manual* at http://www.mysql.com/documentation/index.html.

35.1 CAVEATS

To avoid commonly experienced errors, observe the following caveats about command-line entries:

- `telnet` commands are used to configure SM data and configure or administer users and passwords for `telnet` access to the SSE interface.
- ESNs are entered without dashes in these commands.
- The Canopy system maintains telnet ports in `/etc/services`.
- The SSE port, Port 9080, is aliased as `sse`.

35.2 SSE DATABASE COMMANDS

This section provides the database commands for use with the SSE interface, and defines the allowed usage for each command. At any time, you can enter **`help`** at the `sse` prompt to view these lists.

Distinctive fonts indicate

`literal user input.`
`variable user input.`
`literal system responses.`

`cmd show version`
Display the version of SSE software that is installed.

`cmd show esn`
Display all ESNs with related information. This information includes the cap value and the last `suldr` and `sdldr` values applied to the SM.

`cmd show esn` ***`esn`***
Display the specified ESN (in hexadecimal format without dashes) with related information. ***`esn`*** must be expressed in hexadecimal format.
EXAMPLE: **`cmd show esn 1f2a3f4e3d22`**

cmd show vlanmembers vlanid *vlanid*
List all of the ESNs that are associated with ***vlanid***.
RULES:

vlanid	VLAN ID in the range **1** to **4095**

cmd show config
Display all configuration values that the database uses. This command calls the `show variables` SQL command.
NOTE: This command is deprecated in BAM Release 2.0 and later releases.

cmd show all
Display all configuration values and statistics that are in the database. This command calls the `cmd show config` SSE command.
NOTE: This command is deprecated in BAM Release 2.0 and later releases.

cmd clear esn counter *esn*
Reset the counter to zero for the specified ESN (in hexadecimal format without dashes).
EXAMPLE: **cmd clear esn counter 1f2a3f4e3d22**

config save database */path/filename.txt*
Save the ESN data from the database to the specified path and file.
NOTE: This syntax (**database**) is for execution in only Releases 2.0. The format of SSE database in Releases 1.0 and 1.1 is incompatible with Release 2.0. However, the BAM GUI can be used to import the Release 1.0 or 1.1 format for use with Release 2.0. Using BAM to export the database in Release 2.1 and later is not supported.

config upload database */path/filename.txt*
Upload a properly formatted ESN data file from the specified path to the database.
NOTE: This syntax (**database**) is for execution in only Releases 2.0 and later.

config add esn *esn skey suldr sdldr ulba dlba*
Add the specified ESN with the specified data rates and burst allocations.
RULES:

esn	hexadecimal without dashes. For example, **1f2a3f4e3d22**.
skey	either **0** for the default key or a unique 32-character hexadecimal number for a non-default key.
suldr	**Sustained Uplink Data Rate** in the range **0** to **10000** kbps.
sdldr	**Sustained Downlink Data Rate** in the range **0** to **10000** kbps.
ulba	**Uplink Bandwidth Allocation** in the range **0** to **500000** kbits.
dlba	**Downllink Bandwidth Allocation** in the range **0** to **500000** kbits.

config modify esn *esn* [skey|suldr|sdldr|ulba|dlba][allowhg] *value*
Reset the specified ESN to the specified data rate or burst allocation.
NOTE: This command is for execution in only Releases 2.0 and later. Rules are as defined above.
RULES: All options as above, but also

allowhg request from the license management server a floating Cap 2 (uncapping) license for the SM when the SM registers with **suldr** and **sdldr** values that sum to greater than 7000 kbps, unless the SM already has Cap 2. Value must be either **1** (enable) or **0** (disable).

IMPORTANT!
The following commands suspend or reinstate subscriber access. When you suspend (or reinstate) access by using the BAM SSE command line interface, access is immediately suspended (or reinstated) for the subscriber—a current session is dropped (or registration is now allowed). By contrast, when you suspend (or reinstate) access by selecting **Suspend** (or **Active**) in the BAM GUI, access is not suspended (or reinstated) until the next registration attempt from the subscriber.

config delete esn *esn*
Remove the specified ESN from the database.

config disable esn *esn*
Immediately disable the specified ESN in the database. (See *IMPORTANT* above.)
NOTE: This command is for execution in only Releases 2.0 and later.

config enable esn *esn*
Immediately enable the specified ESN in the database. (See *IMPORTANT* above.)
NOTE: This command is for execution in only Releases 2.0 and later.

config enable esn *esn featurename*
Immediately enable the feature ***featurename*** for the specified ESN.
RULES:

featurename **cir**, **CIR**, **vlan**, or **VLAN**.

config disable esn *esn featurename*
Immediately disable the feature ***featurename*** for the specified ESN. Rules are as defined above.

`config modify esn esn cir [lpruldr|lprdldr|hpruldr|hprdldr|enablehpr] value`
Set or reset the specified CIR parameter for the ESN to the specified value.
RULES:

lpruldr	**Low Priority Uplink CIR** in the range `0` to `20000` kbps.
lprdldr	**Low Priority Downlink CIR** in the range `0` to `20000` kbps.
hpruldr	**High Priority Uplink CIR** in the range `0` to `20000` kbps.
hprdldr	**High Priority Downlink CIR** in the range `0` to `20000` kbps.
enablehpr	**Hi Priority Channel** parameter as `1` (enable) or `0` (disable).

`config modify esn esn vlan [alllearn|allframe|timeout|ingvid|managevid] value`
Set or reset the specified VLAN parameter for the ESN to the specified value.
RULES:

alllearn	**Dynamic Learning** parameter as `1` (enable) or `0` (disable).
allframe	**Allow Only Tagged Frames** parameter as `1` (enable) or `0` (disable).
timeout	**VLAN Aging Timeout** parameter in the range `5` to `1440` minutes.
ingvid	**Untagged Ingress VID** parameter in the range `1` to `4095`.
managevid	**Management VID** parameter in the range `1` to `4095`.

`config add vlanmember esn esn vlanid vlanid`
Associate ***esn*** with the VLAN ***vlanid***.
RULES:

vlanid	`1` to `4095`

`config delete vlanmember esn esn vlanid vlanid`
Dissociate ***esn*** from the VLAN ***vlanid***. Rules are as defined above.

CAUTION!
The following command erases all data in the remote database before the copy execution.

`config copy to database ip user password`
Copy configuration data from port on the network element that is identified by ***ip*** into the database. To do so, identify the ***user*** and ***password*** that the database has stored.
NOTE: This command is deprecated in BAM Release 2.0 and later releases.

35.3 SSE TELNET COMMANDS

This section provides the `telnet` commands for use with the SSE interface, and defines the allowed usage for each command. At any time, the operator can enter **`help`** at the `sse` prompt to view these lists.

Distinctive fonts indicate

`literal user input.`
`variable user input.`

`telnet` ***`localhost`*** **`sse`**
Initiate a telnet session in the SSE interface. The default user name is **`root`**. The default password is **`root`**.

`config add user` ***`user password password`***
Insert a new SSE `telnet` user into the user list. The second instance of ***`password`*** is a required confirmation. By default, a new user is given both read and write access. To restrict access to read-only, use the **`config modify level`** ***`user level`*** command as documented below.

`config delete user` ***`user`***
Remove the specified ***`user`*** from the user list. The user name is required as an argument.

`config store user`
Save changes to the SSE `telnet` user list.

NOTE: (This command is deprecated in BAM Release 2.0 and later releases.)

`config change pass` ***`user password password`***
Change the password for the specified ***`user`*** in the SSE `telnet` user list. The first instance of ***`password`*** is the new password. The second instance of ***`password`*** is a required confirmation of the new password.

`config modify level` ***`user level`***
Change the level of the ***`user`*** from either the default Level 2 or a level previously set by this command. Level 1 allows only read access. Level 2 allows both read and write access. Level 3 allows administrator privileges.

EXAMPLE:
`config modify level patquinn 1`

`help`
Display the full list of supported SSE commands.

`exit`
Conclude and leave the SSE telnet session, but allow the server to continue to operate on software.

36 LEGAL AND REGULATORY NOTICES

36.1 IMPORTANT NOTE ON MODIFICATIONS

Intentional or unintentional changes or modifications to the equipment must not be made unless under the express consent of the party responsible for compliance. Any such modifications could void the user's authority to operate the equipment and will void the manufacturer's warranty.

36.2 NATIONAL AND REGIONAL REGULATORY NOTICES

36.2.1 U.S. Federal Communication Commission (FCC) and Industry Canada (IC) Notification

This device complies with part 15 of the US FCC Rules and Regulations and with RSS-210 of Industry Canada. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) This device must accept any interference received, including interference that may cause undesired operation. In Canada, users should be cautioned to take note that high power radars are allocated as primary users (meaning they have priority) of 5250 – 5350 MHz and 5650 – 5850 MHz and these radars could cause interference and/or damage to license-exempt local area networks (LELAN).

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the US FCC Rules and with RSS-210 of Industry Canada. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with these instructions, may cause harmful interference to radio communications. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment on and off, the user is encouraged to correct the interference by one or more of the following measures:

- Increase the separation between the affected equipment and the unit;
- Connect the affected equipment to a power outlet on a different circuit from that which the receiver is connected to;
- Consult the dealer and/or experienced radio/TV technician for help.
- FCC IDs and Industry Canada Certification Numbers are listed in Table 64:

Table 64: US FCC IDs and Industry Canada Certification Numbers

Module Types	Operating Frequency Range	Maximum Transmitter Power	Reflector or Antenna	FCC ID	Industry Canada Certification Number
SM AP	ISM 902 to 928 MHz	250 mW (24 dBm) 400 mW (26 dBm) 400 mW (26 dBm) 400 mW (26 dBm)	Canopy integrated antenna with 12 dBi gain Maxrad Model # Z1681, flat panel with 10 dBi gain Mars Model # MA-IS91-T2, flat panel with10 dBi gain MTI Model #MT-2630003/N, flat panel with 10 dBi gain	ABZ89FC5809	109W-9000ISM
SM AP BH	ISM 2400-2483.5 MHz	340 mW	Allowed on SM and BH	ABZ89FC5808	109W-2400
SM AP BH	U-NII 5250-5350 MHz	200 mW	Not Allowed	ABZ89FC3789	109W-5200
BH	U-NII 5250-5350 MHz	3.2 mW	Recommended	ABZ89FC5807	109W-5210
SM AP BH	ISM 5725-5850 MHz	200 mW	Allowed on SM and BH	ABZ89FC5804	109W-5700

36.2.2 Regulatory Requirements for CEPT Member States (www.cept.org)

When operated in accordance with the instructions for use, Motorola Canopy Wireless equipment operating in the 2.4 and 5.4 GHz bands is compliant with CEPT Recommendation 70-03 Annex 3 for Wideband Data Transmission and HIPERLANs. For compliant operation in the 2.4 GHz band, the transmit power (EIRP) from the built-in patch antenna and any associated reflector dish shall be no more than 100mW (20dBm). For compliant operation in the 5.4 GHz band, the transmit power (EIRP) from the built-in patch antenna and any associated reflector dish shall be no more than 1 W (30 dBm).

The following countries have completely implemented CEPT Recommendation 70-03 Annex 3A (2.4 GHz band):

- EU & EFTA countries**:** Austria, Belgium, Denmark, Spain, Finland, Germany, Greece, Iceland, Italy, Ireland, Liechtenstein, Luxembourg, Netherlands, Norway, Portugal, Switzerland, Sweden, UK
- New EU member states**:** Czech Republic, Cyprus, Estonia, Hungary, Lithuania, Latvia, Malta, Poland, Slovenia, Slovakia
- Other non-EU & EFTA countries: Bulgaria, Bosnia and Herzegovina, Turkey
- The following countries have a limited implementation of CEPT Recommendation 70-03 Annex 3A:
- France **-** Outdoor operation at 100mW is only permitted in the frequency band 2400 to 2454 MHz;
  - Any outdoor operation in the band 2454 to 2483.5MHz shall not exceed 10mW (10dBm);

- Indoor operation at 100mW (20dBm) is permitted across the band 2400 to 2483.5 MHz
- French Overseas Territories:
  - Guadeloupe, Martinique, St Pierre et Miquelon, Mayotte – 100mW indoor & outdoor is allowed
  - Réunion and Guyana – 100mW indoor, no operation outdoor in the band 2400 to 2420MHz
- Italy - If used outside own premises, general authorization required
- Luxembourg - General authorization required for public service
- Romania - Individual license required. T/R 22-06 not implemented

Motorola Canopy Radios operating in the 2400 to 2483.5MHz band and 5470 to 5725 MHz band are categorized as “Class 2” devices within the EU and are marked with the class identifier symbol, denoting that national restrictions apply (for example, France). The French restriction in the 2.4 GHz band will be removed in 2011. Users are advised to contact their national administrations for the current status on the implementation of ECC DEC(04)08 for the 5.4GHz band.

This equipment is “CE” marked to show compliance with the European Radio & Telecommunications Terminal Equipment (R&TTE) directive 1999/5/EC. The relevant Declaration of Conformity can be found at http://www.canopywireless.com/doc.php.

Where necessary, the end user is responsible for obtaining any National licenses required to operate this product and these must be obtained before using the product in any particular country. However, for CEPT member states, 2.4 GHz Wideband Data Transmission equipment has been designated exempt from individual licensing under decision ERC/DEC(01)07. For EU member states, RLAN equipment in both the 2.4 & 5.4GHz bands is exempt from individual licensing under Commission Recommendation 2003/203/EC. Contact the appropriate national administrations for details on the conditions of use for the bands in question and any exceptions that might apply. Also see www.ero.dk for further information.

36.2.3 European Union Notification

The 5.7 GHz connectorized product is a two-way radio transceiver suitable for use in Broadband Wireless Access System (WAS), Radio Local Area Network (RLAN), or Fixed Wireless Access (FWA) systems. It is a Class 2 device and uses operating frequencies that are not harmonized throughout the EU member states. The operator is responsible for obtaining any national licenses required to operate this product and these must be obtained before using the product in any particular country.

This equipment is marked CE 1321 to show compliance with the European R&TTE directive 1999/5/EC.

The relevant Declaration of Conformity can be found at http://www.canopywireless.com/doc.php.

36.2.4 UK Notification

The 5.7 GHz connectorized product has been notified for operation in the UK, and when operated in accordance with instructions for use it is compliant with UK Interface Requirement IR2007. For UK use, installations must conform to the requirements of IR2007 in terms of EIRP spectral density against elevation profile above the local horizon in order to protect Fixed Satellite Services. The frequency range 5795-5815 MHz is assigned to Road Transport & Traffic Telematics (RTTT) in the U.K. and shall not be used by FWA systems in order to protect RTTT devices. UK Interface Requirement IR2007 specifies that radiolocation services shall be protected by a Dynamic Frequency Selection (DFS) mechanism to prevent co-channel operation in the presence of radar signals.

36.2.5 Belgium Notification

Belgium national restrictions in the 2.4 GHz band include

- EIRP must be lower then 100 mW
- For crossing the public domain over a distance >300m the user must have the authorization of the BIPT.
- No duplex working

36.2.6 Luxembourg Notification

For the 2.4 GHz band, point-to-point or point-to-multipoint operation is only allowed on campus areas. 5.4GHz products can only be used for mobile services.

36.2.7 Czech Republic Notification

This product can be operated in accordance with the Czech General License No. GL-12/R/2000.

36.2.8 Brazil Notification

Local regulations do not allow the use of 900 MHz, 2.4 GHz, 5.2 GHz, or 5.4 GHz Canopy modules in Brazil, nor do they allow the use of passive reflectors on 5.7 GHz Canopy Access Points.

Important Note
This equipment operates as a secondary application, so it has no rights against harmful interference, even if generated by similar equipment, and cannot cause harmful interference on systems operating as primary applications.

36.2.9 Australia Notification

900-MHz modules must be set to transmit and receive only on 919 MHz, 923 MHz or 924 MHz so as to stay within the ACA approved band of 915 MHz to 928 MHz for the class license, given Canopy's 8-MHz channels (at 900 MHz).

After taking into account antenna gain (in dBi), 900 MHz modules transmitter output power (in dBm) must be set to stay within the legal regulatory limit of 30 dBm (1 W) EIRP for this 900-MHz frequency band.

36.3 EXPOSURE

See Preventing Overexposure to RF on Page 127.

36.4 LEGAL NOTICES

36.4.1 Software License Terms and Conditions

ONLY OPEN THE PACKAGE, OR USE THE SOFTWARE AND RELATED PRODUCT IF YOU ACCEPT THE TERMS OF THIS LICENSE. BY BREAKING THE SEAL ON THIS DISK KIT / CDROM, OR IF YOU USE THE SOFTWARE OR RELATED PRODUCT, YOU ACCEPT THE TERMS OF THIS LICENSE AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS, DO NOT USE THE SOFTWARE OR RELATED PRODUCT; INSTEAD, RETURN THE SOFTWARE TO PLACE OF PURCHASE FOR A FULL REFUND. THE FOLLOWING AGREEMENT IS A LEGAL AGREEMENT BETWEEN YOU (EITHER AN INDIVIDUAL OR ENTITY), AND MOTOROLA, INC. (FOR ITSELF AND ITS LICENSORS). THE RIGHT TO USE THIS PRODUCT IS LICENSED ONLY ON THE CONDITION THAT YOU AGREE TO THE FOLLOWING TERMS.

Now, therefore, in consideration of the promises and mutual obligations contained herein, and for other good and valuable consideration, the receipt and sufficiency of which are hereby mutually acknowledged, you and Motorola agree as follows:

Grant of License. Subject to the following terms and conditions, Motorola, Inc., grants to you a personal, revocable, non-assignable, non-transferable, non-exclusive and limited license to use on a single piece of equipment only one copy of the software contained on this disk (which may have been pre-loaded on the equipment)(Software). You may make two copies of the Software, but only for backup, archival, or disaster recovery purposes. On any copy you make of the Software, you must reproduce and include the copyright and other proprietary rights notice contained on the copy we have furnished you of the Software.

Ownership. Motorola (or its supplier) retains all title, ownership and intellectual property rights to the Software and any copies,

including translations, compilations, derivative works (including images) partial copies and portions of updated works. The Software is Motorola's (or its supplier's) confidential proprietary information. This Software License Agreement does not convey to you any interest in or to the Software, but only a limited right of use. You agree not to disclose it or make it available to anyone without Motorola's written authorization. You will exercise no less than reasonable care to protect the Software from unauthorized disclosure. You agree not to disassemble, decompile or reverse engineer, or create derivative works of the Software, except and only to the extent that such activity is expressly permitted by applicable law.

Termination. This License is effective until terminated. This License will terminate immediately without notice from Motorola or judicial resolution if you fail to comply with any provision of this License. Upon such termination you must destroy the Software, all accompanying written materials and all copies thereof, and the sections entitled Limited Warranty, Limitation of Remedies and Damages, and General will survive any termination.

Limited Warranty. Motorola warrants for a period of ninety (90) days from Motorola's or its customer's shipment of the Software to you that (i) the disk(s) on which the Software is recorded will be free from defects in materials and workmanship under normal use and (ii) the Software, under normal use, will perform substantially in accordance with Motorola's published specifications for that release level of the Software. The written materials are provided "AS IS" and without warranty of any kind. Motorola's entire liability and your sole and exclusive remedy for any breach of the foregoing limited warranty will be, at Motorola's option, replacement of the disk(s), provision of downloadable patch or replacement code, or refund of the unused portion of your bargained for contractual benefit up to the amount paid for this Software License.

THIS LIMITED WARRANTY IS THE ONLY WARRANTY PROVIDED BY MOTOROLA, AND MOTOROLA AND ITS LICENSORS EXPRESSLY DISCLAIM ALL OTHER WARRANTIES, EITHER EXPRESS OF IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. MOTOROLA DOES NOT WARRANT THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE, OR THAT DEFECTS IN THE SOFTWARE WILL BE CORRECTED. NO ORAL OR WRITTEN REPRESENTATIONS MADE BY MOTOROLA OR AN AGENT THEREOF SHALL CREATE A WARRANTY OR IN ANY WAY INCREASE THE SCOPE OF THIS WARRANTY. MOTOROLA DOES NOT WARRANT ANY SOFTWARE THAT HAS BEEN OPERATED IN EXCESS OF SPECIFICATIONS, DAMAGED, MISUSED, NEGLECTED, OR IMPROPERLY INSTALLED. BECAUSE SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF IMPLIED WARRANTIES, THE ABOVE LIMITATIONS MAY NOT APPLY TO YOU.

Limitation of Remedies and Damages. Regardless of whether any remedy set forth herein fails of its essential purpose, IN NO EVENT SHALL MOTOROLA OR ANY OF THE LICENSORS, DIRECTORS, OFFICERS, EMPLOYEES OR AFFILIATES OF THE FOREGOING BE LIABLE TO YOU FOR ANY CONSEQUENTIAL, INCIDENTAL, INDIRECT, SPECIAL OR SIMILAR DAMAGES WHATSOEVER (including, without limitation, damages for loss of business profits, business interruption, loss of business information and the like), whether foreseeable or unforeseeable, arising out of the use or inability to use the Software or accompanying written materials, regardless

of the basis of the claim and even if Motorola or a Motorola representative has been advised of the possibility of such damage. Motorola's liability to you for direct damages for any cause whatsoever, regardless of the basis of the form of the action, will be limited to the price paid for the Software that caused the damages. THIS LIMITATION WILL NOT APPLY IN CASE OF PERSONAL INJURY ONLY WHERE AND TO THE EXTENT THAT APPLICABLE LAW REQUIRES SUCH LIABILITY. BECAUSE SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

Maintenance and Support. Motorola shall not be responsible for maintenance or support of the software. By accepting the license granted under this agreement, you agree that Motorola will be under no obligation to provide any support, maintenance or service in connection with the Software or any application developed by you. Any maintenance and support of the Related Product will be provided under the terms of the agreement for the Related Product.

Transfer. In the case of software designed to operate on Motorola equipment, you may not transfer the Software to another party except: (1) if you are an end-user, when you are transferring the Software together with the Motorola equipment on which it operates; or 2) if you are a Motorola licensed distributor, when you are transferring the Software either together with such Motorola equipment or are transferring the Software as a licensed duly paid for upgrade, update, patch, new release, enhancement or replacement of a prior version of the Software. If you are a Motorola licensed distributor, when you are transferring the Software as permitted herein, you agree to transfer the Software with a license agreement having terms and conditions no less restrictive than those contained herein. You may transfer all other Software, not otherwise having an agreed restriction on transfer, to another party. However, all such transfers of Software are strictly subject to the conditions precedent that the other party agrees to accept the terms and conditions of this License, and you destroy any copy of the Software you do not transfer to that party. You may not sublicense or otherwise transfer, rent or lease the Software without our written consent. You may not transfer the Software in violation of any laws, regulations, export controls or economic sanctions imposed by the US Government.

Right to Audit. Motorola shall have the right to audit annually, upon reasonable advance notice and during normal business hours, your records and accounts to determine compliance with the terms of this Agreement.

Export Controls. You specifically acknowledge that the software may be subject to United States and other country export control laws. You shall comply strictly with all requirements of all applicable export control laws and regulations with respect to all such software and materials.

US Government Users. If you are a US Government user, then the Software is provided with "RESTRICTED RIGHTS" as set forth in subparagraphs (c)(1) and (2) of the Commercial Computer Software-Restricted Rights clause at FAR 52 227-19 or subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013, as applicable.

Disputes. You and Motorola hereby agree that any dispute, controversy or claim, except for any dispute, controversy or claim involving intellectual property, prior to initiation of any formal legal process, will be submitted for non-binding mediation, prior to initiation of any formal legal process. Cost of mediation will be shared equally. Nothing in this Section will prevent either party from resorting to judicial proceedings, if (i) good faith efforts to resolve the dispute under these procedures have been unsuccessful, (ii) the dispute, claim or controversy involves intellectual property, or (iii) interim relief from a court is necessary to prevent serious and irreparable injury to that party or to others.

General. Illinois law governs this license. The terms of this license are supplemental to any written agreement executed by both parties regarding this subject and the Software Motorola is to license you under it, and supersedes all previous oral or written communications between us regarding the subject except for such executed agreement. It may not be modified or waived except in writing and signed by an officer or other authorized representative of each party. If any provision is held invalid, all other provisions shall remain valid, unless such invalidity would frustrate the purpose of our agreement. The failure of either party to enforce any rights granted hereunder or to take action

against the other party in the event of any breach hereunder shall not be deemed a waiver by that party as to subsequent enforcement of rights or subsequent action in the event of future breaches.

36.4.2 Hardware Warranty in U.S.

Motorola U.S. offers a warranty covering a period of one year from the date of purchase by the customer. If a product is found defective during the warranty period, Motorola will repair or replace the product with the same or a similar model, which may be a reconditioned unit, without charge for parts or labor.

36.4.3 Limit of Liability

IN NO EVENT SHALL MOTOROLA BE LIABLE TO YOU OR ANY OTHER PARTY FOR ANY DIRECT, INDIRECT, GENERAL, SPECIAL, INCIDENTAL, CONSEQUENTIAL, EXEMPLARY OR OTHER DAMAGE ARISING OUT OF THE USE OR INABILITY TO USE THE PRODUCT (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION OR ANY OTHER PECUNIARY LOSS, OR FROM ANY BREACH OF WARRANTY, EVEN IF MOTOROLA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. (Some states do not allow the exclusion or limitation of incidental or consequential damages, so the above exclusion or limitation may not apply to you.) IN NO CASE SHALL MOTOROLA'S LIABILITY EXCEED THE AMOUNT YOU PAID FOR THE PRODUCT.

37 ADDITIONAL RESOURCES

Canopy provides two additional resources where you can raise questions and find answers:

- Canopy User Community at http://www.canopywireless.com/community.
  This resource facilitates communication with other users and with authorized Canopy experts. Available forums include General Discussion, Network Monitoring Tools, and Suggestions.
- Canopy Knowledge Base at http://www.canopywireless.com/kbase.
  This resource facilitates exploration and searches, provides recommendations, and describes tools. Available categories include
  - General (Answers to general questions provide an overview of the Canopy system.)
  - Product Alerts
  - Helpful Hints
  - FAQs (frequently asked questions)
  - Hardware Support
  - Software Support
  - Tools

38 HISTORY OF DOCUMENTATION

Issue 1 of this *Canopy System User Guide* integrates content from and supersedes

- Issue 5 of the following user manuals:
  - *Canopy Access Point Module (AP) User Manual*
  - *Canopy Backhaul Module (BH) User Manual*
  - *Canopy Subscriber Module (SM) User Manual*
  - *Canopy Cluster Management Module 2 (CMM2) User Manual*
- Issue 3 of the *Canopy Cluster Management Module micro (CMMmicro) User Guide*
- Issue 1 of the *Canopy 900-MHz Access Point (AP) and Subscriber Module (SM) User Guide*
- Issue 2 of the *Canopy Surge Suppressor User Manual*
- Issue 1 of the *Canopy System and Wireless Broadband Terminology Glossary*.

For more information about the change of supporting the radios and CMM2 in this user guide rather than in individual user manuals, see Finding the Information You Need on Page 26.

CANOPY SYSTEM WIRELESS AND BROADBAND TERMINOLOGY GLOSSARY

~.	The command that terminates an SSH Secure Shell session to another server. Used on the Bandwidth and Authentication Manager (BAM) master server in the database replication setup.
10 BaseT	Technology in Ethernet communications that can deliver 10 Mb of data across 328 feet (100 meters) of CAT5 cable.
100 BaseT	Technology in Ethernet communications that can deliver 100 Mb of data across 328 feet (100 meters) of CAT5 cable.
169.254.0.0	Gateway IP address default in Canopy modules.
169.254.1.1	IP address default in Canopy modules.
169.254.x.x	IP address default in Microsoft and Apple operating systems without a DHCP (Dynamic Host Configuration Protocol) server.
255.255.0.0	Subnet mask default in Canopy modules and in Microsoft and Apple operating systems.
802.3	An IEEE standard that defines the contents of frames that are transferred through Ethernet connections. Each of these frames contains a preamble, the address to which the frame is sent, the address that sends the frame, the length of the data to expect, the data, and a checksum to validate that no contents were lost.
Access Point Cluster	Two to six Access Point Modules that together distribute network or Internet services to a community of 1,200 or fewer subscribers. Each Access Point Module covers a 60° sector. This cluster covers as much as 360°. Also known as AP cluster.
Access Point Module	Also known as AP. One module that distributes network or Internet services in a 60° sector to 200 subscribers or fewer.
ACT/4	Second-from-left LED in the module. In the operating mode, this LED is lit when data activity is present on the Ethernet link. In the aiming mode for a Subscriber Module or a Backhaul timing slave, this LED is part of a bar graph that indicates the quality of the RF link.
Activate	To provide feature capability to a module, but not to *enable* (turn on) the feature in the module. See also Enable.
Address Resolution Protocol	Protocol defined in RFC 826 to allow a network element to correlate a host IP address to the Ethernet address of the host. See http://www.faqs.org/rfcs/rfc826.html.
Advanced Encryption Standard	Over-the-air link option that provides extremely secure wireless connections. Advanced Encryption Standard (AES) uses 128-bit secret keys as directed by the government of the U.S.A. AES is not exportable and requires a special AP to process the large keys.

AES	Advanced Encryption Standard. An over-the-air link option that provides extremely secure wireless connections. AES uses 128-bit secret keys as directed by the government of the U.S.A. AES is not exportable and requires a special AP to process the large keys.
AP	Access Point Module. One module that distributes network or Internet services in a 60° sector to 200 subscribers or fewer.
APA	Access Point module address.
Apache	A trademark of Apache Software Foundation, used with permission.
APAS	Status page indication that confirms that authentication is *active* for the AP. However, this indication does not confirm that authentication is *enabled* (turned on) for the AP. See also Activate and Enable.
APs MIB	Management Information Base file that defines objects that are specific to the Access Point Module or Backhaul timing master. See also Management Information Base.
ARP	Address Resolution Protocol. A protocol defined in RFC 826 to allow a network element to correlate a host IP address to the Ethernet address of the host. See http://www.faqs.org/rfcs/rfc826.html.
ASN.1	Abstract Syntax Notation One language. The format of the text files that compose the Management Information Base.
Attenuation	Reduction of signal strength caused by the travel from the transmitter to the receiver, and caused by any object between. In the absence of objects between, a signal that has a short wavelength experiences a high degree of attenuation nevertheless.
Authentication Key	Software key that correlates to the random number that the Bandwidth and Authentication Manager (BAM) server generates and sends in a challenge through the AP to the SM. The network operator can create and, at some security risk, send this key over the air to the SM. The SQL database in the BAM server correlates this key to QoS information about the SM. The format of this key is 32 hexadecimal characters of 0 to 9 and a to f, padded with leading zeroes in Release 4.2.3 and later releases. This key must be unique to the individual SM.
Authorization Key Field	Name of the parameter that identifies the *authentication* key in the SM Configuration web page. See Authentication Key or skey.
Backhaul Module	Also known as BH. A module that provides point-to-point connectivity as either a standalone link or a link to an Access Point cluster through a selected Access Point Module. See also Backhaul Timing Master and Backhaul Timing Slave.
Backhaul Timing Master	Backhaul Module that sends network timing (synchronization) to another Backhaul Module, which serves as the Backhaul timing slave.

Backhaul Timing Slave	Backhaul Module that receives network timing (synchronization) from another Backhaul Module, which serves as the Backhaul timing master.
BAM	Bandwidth and Authentication Manager. Software that operates on a Linux server to manage data rate and burst data capabilities individually for each registered Subscriber Module. This software also provides secure Subscriber Module authentication and user-specified encryption keys.
Bandwidth and Authentication Manager	Software that operates on a Linux server to manage data rate and burst data capabilities individually for each registered Subscriber Module. This software also provides secure Subscriber Module authentication and user-specified encryption keys.
BER	Bit Error Rate. The ratio of incorrect data received to correct data received.
BH	Backhaul Module. A module that provides point-to-point connectivity as either a standalone link or a link to an Access Point cluster through a selected Access Point Module.
Bit Error Rate	Ratio of incorrect data received to correct data received.
Box MIB	Management Information Base file that defines module-level objects. See also Management Information Base.
BRAID	Stream cipher that the TIA (Telecommunications Industry Association) has standardized. The secret keys in both modules communicate with each other to establish the Data Encryption Standard key. See Data Encryption Standard.
Bridge	Network element that uses the physical address (not the logical address) of another to pass data. The bridge passes the data to either the destination address, if found in the simple routing table, or to all network segments other than the one that transmitted the data. Canopy modules are Layer 2 bridges except that, where NAT is enabled for an SM, the SM is a Layer 3 switch. Compare to Switch and Router, and see also NAT.
Bridge Entry Timeout Field	Value that the operator sets as the maximum interval for no activity with another module, whose MAC address is the Bridge Entry. This interval should be longer than the ARP (Address Resolution Protocol) cache timeout of the router that feeds the network.
Buckets	Theoretical data repositories that can be filled at preset rates or emptied when preset conditions are experienced, such as when data is transferred.
Burst	Preset amount limit of data that may be continuously transferred.
C/I Ratio	Ratio of intended reception to unintended reception.

Canopy	A trademark of Motorola, Inc.
canopy.xml	File that stores specifications for the Bandwidth and Authentication Manager (BAM) GUI.
Carrier-to-interference Ratio	Ratio of intended reception to unintended reception.
CarSenseLost Field	This field displays how many carrier sense lost errors occurred on the Ethernet controller.
CAT5 Cable	Cable that delivers Ethernet communications from module to module. Later modules auto-sense whether this cable is wired in a straight-through or crossover scheme.
cdf	Canopy Data Formatter tool that creates an initial ESN Data Table. Inputs for this tool include a list of SM ESNs and default values of sustained data rates and burst allocations for each listed ESN.
chkconfig	A command that the Linux® operating system accepts to enable MySQL® and Apache™ Server software for various run levels of the mysqld and httpd utilities.
Cluster Management Module	Module that provides power, GPS timing, and networking connections for an AP cluster. Also known as CMM. If this CMM is connected to a Backhaul Module, then this CMM is the central point of connectivity for the entire site.
CMM	Cluster Management Module. A module that provides power, GPS timing, and networking connections for an Access Point cluster. If this CMM is connected to a Backhaul Module (BH), then this CMM is the central point of connectivity for the entire site.
Color Code Field	Module parameter that identifies the other modules with which communication is allowed. The range of values is 0 to 255. When set at 0, the Color Code does not restrict communications with any other module.
Community String Field	Control string that allows a network management station to access MIB information about the module.
CPE	Customer premises equipment.
CRCError Field	This field displays how many CRC errors occurred on the Ethernet controller.
Data Encryption Standard	Over-the-air link option that uses secret 56-bit keys and 8 parity bits. Data Encryption Standard (DES) performs a series of bit permutations, substitutions, and recombination operations on blocks of data.

Date of Last Transaction A field in the data that the `cmd show esn` command generates from data in the SQL database in the Bandwidth and Authentication Manager (BAM) server. This field identifies the date of the most recent authentication attempt by the SM. Expressed in the database output as DLT.

Dell A trademark of Dell, Inc.

Demilitarized Zone Internet Protocol area outside of a firewall. Defined in RFC 2647. See http://www.faqs.org/rfcs/rfc2647.html.

DES Data Encryption Standard. An over-the-air link option that uses secret 56-bit keys and 8 parity bits. DES performs a series of bit permutations, substitutions, and recombination operations on blocks of data.

Desensed Received an undesired signal that was strong enough to make the module insensitive to the desired signal.

DHCP Dynamic Host Configuration Protocol, defined in RFC 2131. Protocol that enables a device to be assigned a new IP address and TCP/IP parameters, including a default gateway, whenever the device reboots. Thus DHCP reduces configuration time, conserves IP addresses, and allows modules to be moved to a different network within the Canopy system. See http://www.faqs.org/rfcs/rfc2131.html. See also Static IP Address Assignment.

Diffraction Partial obstruction of a signal. Typically diffraction attenuates a signal so much that the link is unacceptable. However, in some instances where the obstruction is very close to the receiver, the link may be acceptable.

Disable To turn off a feature in the module after both the feature activation file has *activated* the module to use the feature and the operator has *enabled* the feature in the module. See also Activate and Enable.

DLT Date of last transaction. A field in the data that the `cmd show esn` command generates from data in the SQL database in the Bandwidth and Authentication Manager (BAM) server. This field identifies the date of the most recent authentication attempt by the SM.

DMZ Demilitarized Zone as defined in RFC 2647. An Internet Protocol area outside of a firewall. See http://www.faqs.org/rfcs/rfc2647.html.

Dynamic Host Configuration Protocol Protocol defined in RFC 2131 that enables a device to be assigned a new IP address and TCP/IP parameters, including a default gateway, whenever the device reboots. Thus Dynamic Host Configuration Protocol reduces configuration time, conserves IP addresses, and allows modules to be moved to a different network within the Canopy system. See http://www.faqs.org/rfcs/rfc2131.html. See also Static IP Address Assignment.

Electronic Serial Number	Hardware address that the factory assigns to the module for identification in the Data Link layer interface of the Open Systems Interconnection system. This address serves as an electronic serial number. Same as MAC Address.
Enable	To turn on a feature in the module after the feature activation file has *activated* the module to use the feature. See also Activate.
Engine	Bandwidth and Authentication Manager (BAM) interface to the AP and SMs. Unique sets of commands are available on this interface to manage parameters and user access. Distinguished from SSE. See also SSE.
ESN	Electronic Serial Number. The hardware address that the factory assigns to the module for identification in the Data Link layer interface of the Open Systems Interconnection system. This address serves as an electronic serial number. Same as MAC Address.
ESN Data Table	Table in which each row identifies data about a single SM. In tab-separated fields, each row stores the ESN, authentication key, and QoS information that apply to the SM. The operator can create and modify this table. This table is both an input to and an output from the Bandwidth and Authentication Manager (BAM) SQL database, and should be identically input to redundant BAM servers.
/etc/services	File that stores telnet ports on the Bandwidth and Authentication Manager (BAM) server.
EthBusErr Field	This field displays how many Ethernet bus errors occurred on the Ethernet controller.
Ethernet Protocol	Any of several IEEE standards that define the contents of frames that are transferred from one network element to another through Ethernet connections.
FCC	Federal Communications Commission of the U.S.A.
Feature Activation Key	Software key file whose file name includes the ESN of the target Canopy module. When installed on the module, this file *activates* the module to have the feature *enabled* or disabled in a separate operator action.
Field-programmable Gate Array	Array of logic, relational data, and wiring data that is factory programmed and can be reprogrammed.
File Transfer Protocol	Utility that transfers of files through TCP (Transport Control Protocol) between computing devices that do not operate on the same platform. Defined in RFC 959. See http://www.faqs.org/rfcs/rfc959.html.
FPGA	Field-programmable Gate Array. An array of logic, relational data, and wiring data that is factory programmed and can be reprogrammed.

Frame Spreading	Transmission of a beacon in only frames where the receiver expects a beacon (rather than in every frame). This avoids interference from transmissions that are not intended for the receiver.
Frame Timing Pulse Gated Field	Toggle parameter that prevents or allows the module to continue to propagate GPS sync timing when the module no longer receives the timing.
Free Space Path Loss	Signal attenuation that is naturally caused by atmospheric conditions and by the distance between the antenna and the receiver.
Fresnel Zone	Space in which no object should exist that can attenuate, diffract, or reflect a transmitted signal before the signal reaches the target receiver.
FSK	Frequency Shift Keying, a variation of frequency modulation to transmit data, in which two or more frequencies are used.
FTP	File Transfer Protocol, defined in RFC 959. Utility that transfers of files through TCP (Transport Control Protocol) between computing devices that do not operate on the same platform. See http://www.faqs.org/rfcs/rfc959.html.
Global Positioning System	Network of satellites that provides absolute time to networks on earth, which use the time signal to synchronize transmission and reception cycles (to avoid interference) and to provide reference for troubleshooting activities.
GPS	Global Positioning System. A network of satellites that provides absolute time to networks on earth, which use the time signal to synchronize transmission and reception cycles (to avoid interference) and to provide reference for troubleshooting activities.
GPS/3	Third-from-left LED in the module. In the operating mode for an Access Point Module or Backhaul timing master, this LED is continuously lit as the module receives sync pulse. In the operating mode for a Subscriber Module or a Backhaul timing slave, this LED flashes on and off to indicate that the module is not registered. In the aiming mode for a Subscriber Module or a Backhaul timing slave, this LED is part of a bar graph that indicates the quality of the RF link.
Graphical Internet	A Red Hat® Linux® 9 operating system package group that enables the Bandwidth and Authentication Manager (BAM) GUI.
GUI	Graphical user interface.
High-priority Channel	Channel that supports low-latency traffic (such as Voice over IP) over low-latency traffic (such as standard web traffic and file downloads). To recognize the latency tolerance of traffic, this channel reads the IPv4 Type of Service Low Latency bit.

HTTP	Hypertext Transfer Protocol, used to make the Internet resources available on the World Wide Web. Defined in RFC 2068. See http://www.faqs.org/rfcs/rfc2068.html.
ICMP	Internet Control Message Protocols defined in RFC 792, used to identify Internet Protocol (IP)-level problems and to allow IP links to be tested. See http://www.faqs.org/rfcs/rfc792.html.
indiscards count Field	How many inbound packets were discarded without errors that would have prevented their delivery to a higher-layer protocol. (Some of these packets may have been discarded to increase buffer space.)
inerrors count Field	How many inbound packets contained errors that prevented their delivery to a higher-layer protocol.
innucastpkts count Field	How many inbound non-unicast (subnetwork-broadcast or subnetwork-multicast) packets were delivered to a higher-layer protocol.
inoctets count Field	How many octets were received on the interface, including those that deliver framing information.
Intel	A registered trademark of Intel Corporation.
inucastpkts count Field	How many inbound subnetwork-unicast packets were delivered to a higher-layer protocol.
inunknownprotos count Field	How many inbound packets were discarded because of an unknown or unsupported protocol.
IP	Internet Protocol defined in RFC 791. The Network Layer in the TCP/IP protocol stack. This protocol is applied to addressing, routing, and delivering, and re-assembling data packets into the Data Link layer of the protocol stack. See http://www.faqs.org/rfcs/rfc791.html.
IP Address	32-bit binary number that identifies a network element by both network and host. See also Subnet Mask.
IPv4	Traditional version of Internet Protocol, which defines 32-bit fields for data transmission.
ISM	Industrial, Scientific, and Medical Equipment radio frequency band, in the 900-MHz, 2.4-GHz, and 5.8-GHz ranges.
Jitter	Timing-based measure of the reception quality of a link. An acceptable link displays a jitter value between 0 and 4 for a 10-Mbps Backhaul timing slave in Release 4.0 and later releases, between 0 and 9 for a 20-Mbps Backhaul timing slave, or between 5 and 9 for any Subscriber Module or for a Backhaul timing slave in any earlier release.

Late Collision Field	This field displays how many late collisions occurred on the Ethernet controller. A normal collision occurs during the first 512 bits of the frame transmission. A collision that occurs after the first 512 bits is considered a late collision. A late collision is a serious network problem because the frame being transmitted is discarded. A late collision is most commonly caused by a mismatch between duplex configurations at the ends of a link segment.
Latency Tolerance	Acceptable tolerance for delay in the transfer of data to and from a module.
Line of Sight	Wireless path (not simply visual path) direct from module to module. The path that results provides both ideal aim and an ideal Fresnel zone.
Linux	A registered trademark of Linus Torvalds.
LNK/5	Furthest left LED in the module. In the operating mode, this LED is continuously lit when the Ethernet link is present. In the aiming mode for a Subscriber Module or a Backhaul timing slave, this LED is part of a bar graph that indicates the quality of the RF link.
Logical Unit ID	Final octet of the 4-octet IP address of the module.
LOS	Line of sight. The wireless path (not simply visual path) direct from module to module. The path that results provides both ideal aim and an ideal Fresnel zone.
LUID	Logical Unit ID. The final octet of the 4-octet IP address of the module.
MAC Address	Media Access Control address. The hardware address that the factory assigns to the module for identification in the Data Link layer interface of the Open Systems Interconnection system. This address serves as an electronic serial number.
Management Information Base	Space that allows a program (agent) in the network to relay information to a network monitor about the status of defined variables (objects).
Master	Designation that defines the role of a component relative to the role of another. This designation both applies to a Backhaul module that provides synchronization over the air to another Backhaul module (a Backhaul timing slave) and applies to a Bandwidth and Authentication Manager (BAM) server whose SQL database is automatically copied onto a redundant BAM server (BAM slave). In each case, the master is not a product. Rather, the master is the role that results from deliberate configuration steps.
Media Access Control Address	Hardware address that the factory assigns to the module for identification in the Data Link layer interface of the Open Systems Interconnection system. This address serves as an electronic serial number.

MIB	Management Information Base. Space that allows a program (agent) in the network to relay information to a network monitor about the status of defined variables (objects).
MySQL	A registered trademark of MySQL AB Company in the United States, the European Union, and other countries.
mysqladmin	A command to set the administrator and associated password on the Bandwidth and Authentication Manager (BAM) server.
mysql-server	Package group that enables the SQL Database Server application in the Red Hat® Linux® 9 operating system to provide SQL data for Bandwidth and Authentication Manager (BAM) operations.
NAT	Network Address Translation defined in RFC 1631. A scheme that isolates Subscriber Modules from the Internet. See http://www.faqs.org/rfcs/rfc1631.html.
NEC	National Electrical Code. The set of national wiring standards that are enforced in the U.S.A.
NetBIOS	Protocol defined in RFC 1001 and RFC 1002 to support an applications programming interface in TCP/IP. This interface allows a computer to transmit and receive data with another host computer on the network. RFC 1001 defines the concepts and methods. RFC 1002 defines the detailed specifications. See http://www.faqs.org/rfcs/rfc1001.html and http://www.faqs.org/rfcs/rfc1002.html.
Network Address Translation	Scheme that defines the Access Point Module as a proxy server to isolate registered Subscriber Modules from the Internet. Defined in RFC 1631. See http://www.faqs.org/rfcs/rfc1631.html.
Network Management Station	Monitor device that uses Simple Network Management Protocol (SNMP) to control, gather, and report information about predefined network variables (objects).
NMS	Network Management Station. A monitor device that uses Simple Network Management Protocol (SNMP) to control, gather, and report information about predefined network variables (objects).
Object	Network variable that is defined in the Management Information Base.
OptiPlex	A trademark of Dell, Inc.
outdiscards count Field	How many outbound packets were discarded without errors that would have prevented their transmission. (Some of these packets may have been discarded to increase buffer space.)
outerrrors count Field	How many outbound packets contained errors that prevented their transmission.

outnucastpkts count Field	How many packets for which the higher-level protocols requested transmission to a non-unicast (subnetwork-broadcast or subnetwork-multicast) address. The number includes those that were discarded or not sent.
outoctets count Field	How many octets were transmitted out of the interface, including those that deliver framing information.
outucastpkts count Field	How many packets for which the higher-level protocols requested transmission to a subnetwork-unicast address. The number includes those that were discarded or not sent.
Override Plug	Device that enables the operator to regain control of a module that has been locked by the No Remote Access feature, the 802.3 Link Disable feature, or a password or IP address that cannot be recalled. This device can be either fabricated on site or ordered.
Pentium	A registered trademark of Intel Corporation.
php-mysql	Package group that enables the Web Server application in the Red Hat® Linux® 9 operating system to provide data from the SQL Database Server application as PHP in the Bandwidth and Authentication Manager (BAM) GUI.
Point-to-Point Protocol	Standards that RFC 1661 defines for data transmittal on the Internet. Also known as PPP or PTP. See http://www.faqs.org/rfcs/rfc1661.html.
Power Control	Feature in Release 4.1 and later releases that allows the module to operate at less than 18 dB less than full power to reduce self-interference.
Protective Earth	Connection to earth (which has a charge of 0 volts). Also known as ground.
Proxy Server	Network computer that isolates another from the Internet. The proxy server communicates for the other computer, and sends replies to only the appropriate computer, which has an IP address that is not unique or not registered.
PTMP	Point-to-Multipoint Protocol defined in RFC 2178, which specifies that data that originates from a central network element can be received by all other network elements, but data that originates from a non-central network element can be received by only the central network element. See http://www.faqs.org/rfcs/rfc2178.html.
PTP	Point-to-Point Protocol. The standards that RFC 1661 defines for data transmittal on the Internet. See http://www.faqs.org/rfcs/rfc1661.html.

QoS Quality of Service. A frame field that Bandwidth and Authentication Manager (BAM) provides to the AP and SM the sustained data rates and burst data limits of the SM. The format of this field is 64 hexadecimal characters of 0 to 9 and a to f. The BAM SQL database expresses this field as five contiguous subfields.

Quality of Service A frame bit that Bandwidth and Authentication Manager (BAM) provides to the AP and SM the sustained data rates and burst data limits of the SM. The format of this field is 64 hexadecimal characters of 0 to 9 and a to f. The BAM SQL database expresses this field as five contiguous subfields. Also known as QoS.

Quick Start Interface page that requires minimal configuration for initial module operation.

Radio Signal Strength Indicator Relative measure of the strength of a received signal. An acceptable link displays an Radio Signal Strength Indicator (RSSI) value of greater than 700.

Random Number Number that the Bandwidth and Authentication Manager (BAM) generates, invisible to both the SM and the network operator, to send to the SM as a challenge against an authentication attempt.

Reader A registered trademark of Adobe Systems, Incorporated.

Recharging Resumed accumulation of data in available data space (buckets). See Buckets.

Red Hat A registered trademark of Red Hat, Inc.

Reflection Change of direction and reduction of amplitude of a signal that encounters an object larger than the wavelength. Reflection may cause an additional copy of the wavelength to arrive at after the original, unobstructed wavelength arrives. This causes partial cancellation of the signal and may render the link unacceptable. However, in some instances where the direct signal cannot be received, the reflected copy may be received and render an otherwise unacceptable link acceptable.

Registrations MIB Management Information Base file that defines registrations for global items such as product identities and product components. See also Management Information Base.

repl-m A command that sets up the database replication process on a Bandwidth and Authentication Manager (BAM) master server, uses SFTP to copy both the database and the `repl-s` script to a BAM slave server, and remotely executes the `repl-s` script on the BAM slave server. See Master, Slave, `repl-s`, Secure Shell, and SFTP.

repl-s A command that sets up the database replication process on a Bandwidth and Authentication Manager (BAM) slave server. See Master, Slave, and `repl-m`.

RES Result. A field in the data that the `cmd show esn` command generates from the SQL database in the Bandwidth and Authentication Manager (BAM) server.

RetransLimitExp Field This field displays how many times the retransmit limit has expired.

RF Radio frequency. How many times each second a cycle in the antenna occurs, from positive to negative and back to positive amplitude.

RJ-11 Standard cable that is typically used for telephone line or modem connection.

RJ-45 Standard cable that is typically used for Ethernet connection. This cable may be wired as straight-through or as crossover. Later Canopy modules auto-sense whether the cable is straight-through or crossover.

Router Network element that uses the logical (IP) address of another to pass data to only the intended recipient. Compare to Switch and Bridge.

RPM Red Hat® Package Manager.

rpm A command that the Linux® operating system accepts to identify the version of Linux® software that operates on the Bandwidth and Authentication Manager (BAM) server.

RSSI Radio Signal Strength Indicator. A relative measure of the strength of a received signal. An acceptable link displays an RSSI value of greater than 700.

RxBabErr Field This field displays how many receiver babble errors occurred.

RxOverrun Field This field displays how many receiver overrun errors occurred on the Ethernet controller.

Secure Shell A trademark of SSH Communications Security.

Self-interference Interference with a module from another module in the same network.

SES/2 Third-from-right LED in the module. In the Access Point Module and Backhaul timing master, this LED is unused. In the operating mode for a Subscriber Module or a Backhaul timing slave, this LED flashes on and off to indicate that the module is not registered. In the aiming mode for a Subscriber Module or a Backhaul timing slave, this LED is part of a bar graph that indicates the quality of the RF link.

Session Key Software key that the SM and Bandwidth and Authentication Manager (BAM) separately calculate based on that both the authentication key (or the factory-set default key) and the random number. BAM sends the session key to the AP. Neither the subscriber nor the network operator can view this key. See also Random Number.

SFTP	Secure File Transfer Protocol.
Simple Network Management Protocol	Standard that is used for communications between a program (agent) in the network and a network management station (monitor). Defined in RFC 1157. See http://www.faqs.org/rfcs/rfc1157.html.
skey	Software key that correlates to the random number that the Bandwidth and Authentication Manager (BAM) server generates and sends in a challenge through the AP to the SM. The network operator can create and, at some security risk, send this key over the air to the SM. The SQL database in the BAM server correlates this key to QoS information about the SM. The format of this key is 32 hexadecimal characters of 0 to 9 and a to f. This key must be unique to the individual SM. Also known as authentication key.
Slave	Designation that defines the role of a component relative to the role of another. This designation both applies to a Backhaul slave that receives synchronization over the air from another Backhaul module (a Backhaul timing master) and applies to a redundant Bandwidth and Authentication Manager (BAM) server whose SQL database is automatically overwritten by a copy from the primary BAM server (BAM master). In each case, the slave is not a product. Rather, the slave is the role that results from deliberate configuration steps.
SM	Customer premises equipment (CPE) device that extends network or Internet services by communication with an Access Point Module or an Access Point cluster.
SM MIB	Management Information Base file that defines objects that are specific to the Subscriber Module or Backhaul timing slave. See also Management Information Base.
SNMP	Simple Network Management Protocol, defined in RFC 1157. A standard that is used for communications between a program (agent) in the network and a network management station (monitor). See http://www.faqs.org/rfcs/rfc1157.html.
SNMP Trap	Capture of information that informs the network monitor through Simple Network Management Protocol of a monitored occurrence in the module.
SSE	Bandwidth and Authentication Manager (BAM) interface to the SQL server. Unique sets of commands are available on this interface to manage the BAM SQL database and user access. Distinguished from Engine. See also Engine.
Static IP Address Assignment	Assignment of Internet Protocol address that can be changed only manually. Thus static IP address assignment requires more configuration time and consumes more of the available IP addresses than DHCP address assignment does. RFC 2050 provides guidelines for the static allocation of IP addresses. See http://www.faqs.org/rfcs/rfc2050.html. See also DHCP.

su - A command that opens a Linux® operating system session for the user `root`.

Subnet Mask 32-bit binary number that filters an IP address to reveal what part identifies the network and what part identifies the host. The number of subnet mask bits that are set to 1 indicates how many leading bits of the IP address identify the network. The number of subnet mask bits that are set 0 indicate how many trailing bits of the IP address identify the host.

Subscriber Module Customer premises equipment (CPE) device that extends network or Internet services by communication with an Access Point Module or an Access Point cluster.

Sustained Data Rate Preset rate limit of data transfer.

Switch Network element that uses the port that is associated with the physical address of another to pass data to only the intended recipient. Compare to Bridge and Router.

SYN/1 Second-from-right LED in the module. In the Access Point Module or Backhaul timing master, as in a registered Subscriber Module or Backhaul timing slave, this LED is continuously lit to indicate the presence of sync. In the operating mode for a Subscriber Module or Backhaul timing slave, this LED flashes on and to indicate that the module is not registered. In the aiming mode for a Subscriber Module or a Backhaul timing slave, this LED is part of a bar graph that indicates the quality of the RF link.

Sync GPS (Global Positioning System) absolute time, which is passed from one module to another. Sync enables timing that prevents modules from transmitting or receiving interference. Sync also provides correlative time stamps for troubleshooting efforts.

TCP Alternatively known as Transmission Control Protocol or Transport Control Protocol. The Transport Layer in the TCP/IP protocol stack. This protocol is applied to assure that data packets arrive at the target network element and to control the flow of data through the Internet. Defined in RFC 793. See http://www.faqs.org/rfcs/rfc793.html.

tcp Transport Control type of port. The Canopy system uses Port 3306:tcp for MySQL® database communications, Port 9080:tcp for SSE `telnet` communications, and Port 9090:tcp for Engine `telnet` communications.

TDD Time Division Duplexing.

TDMA Time Division Multiple Access.

telnet	Utility that allows a client computer to update a server. A firewall can prevent the use of the `telnet` utility to breach the security of the server. See http://www.faqs.org/rfcs/rfc818.html, http://www.faqs.org/rfcs/rfc854.html and http://www.faqs.org/rfcs/rfc855.html.
Textual Conventions MIB	Management Information Base file that defines Canopy system-specific textual conventions. See also Management Information Base.
Time of Last Transaction	A field in the data that the `cmd show esn` command generates from data in the SQL database in the Bandwidth and Authentication Manager (BAM) server. This field identifies the time of day of the most recent authentication attempt by the SM. Expressed in the database output as TLT.
TLT	Time of last transaction. A field in the data that the `cmd show esn` command generates from data in the SQL database in the Bandwidth and Authentication Manager (BAM) server. This field identifies the time of day of the most recent authentication attempt by the SM.
TNAF	Total number of authentication requests failed. A field in the data that the `cmd show esn` command generates from the SQL database in the Bandwidth and Authentication Manager (BAM) server. This field indicates how many times the SM (identified by ESN in the related data) attempted to authenticate but was denied by BAM.
TNAR	Total number of authentication requests. A field in the data that the `cmd show esn` command generates from the SQL database in the Bandwidth and Authentication Manager (BAM) server. This field indicates how many times the SM (identified by ESN in the related data) attempted to authenticate, regardless of whether the attempt succeeded.
Tokens	Theoretical amounts of data. See also Buckets.
TOS	8-bit field in that prioritizes data in a IP transmission. See http://www.faqs.org/rfcs/rfc1349.html.
TxUnderrun Field	This field displays how many transmission-underrun errors occurred on the Ethernet controller.
UDP	User Datagram Protocol. A set of Network, Transport, and Session Layer protocols that RFC 768 defines. These protocols include checksum and address information but does not retransmit data or process any errors. See http://www.faqs.org/rfcs/rfc768.html.
udp	User-defined type of port.
U-NII	Unlicensed National Information Infrastructure radio frequency band, in the 5.1-GHz through 5.8-GHz ranges.